مرکز صدور گواهی الکترونیکی پارس‌ساین

راهنمای استفاده از گواهی الکترونیکی در نرم‌افزار

Microsoft IIS 7

تدوین‌کننده: شرکت امن‌افزار گستر شریف

شمارهٔ سند.....SSW_UG_PKI_91109_1

تاریخ..... ۰۲/مرداد/۱۳۹۲

نگارش..... ۱.۸

آدرس: تهران، خیابان آزادی، خیابان حبیب‌الله، خیابان قاسمی غربی، نبش بن‌بست پیام آزادی، شمارهٔ ۳۷، طبقه پنجم

تلفن: ۲۰-۶۱۹۷۵۵۰۰ (۰۲۱) **فاکس:** ۶۶۰۹۰۲۹۹ (۰۲۱) **سایت اینترنتی:** www.parssignca.ir

حق طبع و نشر

فهرست مطالب

۱ مقدمه

تأمین امنیت ارتباطات و تبادلات الکترونیکی در شبکه‌ها خصوصاً محیط اینترنت از جمله مسائل ویژه‌ای است که امروزه سازمان‌ها با آن مواجه هستند. به دلیل حساسیت امنیتی حجم قابل توجهی از این تبادلات در محیط وب، باید تدابیر امنیتی لازم در پروتکل‌ها و سرویس‌های مورد استفاده در این نوع ارتباطات اتخاذ گردد. پروتکل HTTP (که عموماً به عنوان پروتکل وب شناخته می‌شود) یکی از این پروتکل‌ها است که استفاده گسترده‌ای دارد. داده‌های HTTP به صورت ناامن روی شبکه منتقل می‌شوند؛ از این‌رو، داده‌هایی که بین سرویس‌دهنده[1] (سمت وب‌سایت) و سرویس‌گیرنده[2] (سمت کاربر وب‌سایت) مبادله می‌شود، توسط مهاجمین قابل مشاهده و حتی قابل تغییر هستند.

وب‌سایت‌هایی که اطلاعات مهم و محرمانه (مانند گذرواژه، شماره کارت اعتباری، اطلاعات بانکی، و دیگر اطلاعات خصوصی) با کاربران مبادله می‌کنند، نباید از پروتکل ناامن HTTP استفاده نمایند. نسخه امن‌شده این پروتکل به نام HTTPS، پرکاربردترین پروتکل امنیتی مبتنی بر رمزنگاری کلید عمومی است که در پیاده‌سازی این گونه وب‌سایت‌ها به کار می‌رود. این پروتکل مبتنی بر پروتکل SSL می‌باشد.

لازم به ذکر است، تأمین محرمانگی و عدم تغییر (جامعیت) اطلاعات تبادل‌شده بین کاربر و وب‌سایت تنها کاربرد HTTPS نیست. HTTPS برای جلوگیری از حملاتی مانند حمله فیشینگ مبتنی بر جعل سایت نیز استفاده می‌شود. در حمله مذکور، حمله‌کننده (مثلاً یک رقیب تجاری) با ایجاد یک وب‌سایت با ظاهری کاملاً مشابه سایت اصلی، کاربران آن سایت را به سایت جعلی هدایت کرده و امنیت آن‌ها را به مخاطره می‌اندازد؛ مثلاً اطلاعات کاربران را به سرقت می‌برد یا در مورد آن‌ها اطلاعات جمع‌آوری می‌کند. در صورتی که از گواهی HTTPS استفاده شود، از این حمله جلوگیری می‌شود.

در پیکربندی وب سرور برای استفاده از HTTPS، از یک گواهی الکترونیکی SSL استفاده می‌شود. این گواهی باید توسط یک مرکز صدور گواهی الکترونیکی معتبر (مانند مرکز صدور گواهی الکترونیکی پارس‌ساین) صادر شده باشد تا کاربران بتوانند به آن اعتماد کرده و اطلاعات محرمانه خود را بر اساس این اعتماد، برای وب‌سایت ارسال نمایند.

---

[1] Server
[2] Client

در این سند، کلیه مراحل لازم برای پیکربندی وب‌سرور Microsoft IIS 7 به منظور استفاده از گواهی SSL توضیح داده شده است. لازم به ذکر است، رویه برای نسخه‌های دیگر IIS نیز تقریباً مشابه است.

۲ فرضیات این سند

در این سند، نحوه استفاده از گواهی الکترونیکی، بر اساس سناریوی فرضی زیر در نظر گرفته شده است:

«برای یک وب‌سایت به آدرس www.mydomain.com، می‌خواهیم از مرکز صدور گواهی الکترونیکی پارس‌ساین، گواهی SSL درخواست نماییم. پس از دریافت گواهی، فایل گواهی به فرمت PFX را ایجاد نموده و آن را در نرم‌افزار Microsoft IIS 7 به وب‌سایت مورد نظر تخصیص دهیم. سپس وب سرور را طوری تنظیم نماییم که امکان برقراری ارتباط HTTPS با آن فراهم شود».

از این‌رو، به منظور استفاده از این سند در سناریوی واقعی، باید به موارد زیر دقت نمایید:

- به جای آدرس www.mydomain.com، باید از آدرس دقیق وب‌سایتی استفاده نمایید که برای آن گواهی SSL درخواست نموده‌اید.
- در مثال فرضی ما، وب‌سایت پیش‌فرض (Default Web Site) در وب‌سرور IIS، سایت www.mydomain.com می‌باشد. از آنجا که ممکن است همیشه این‌گونه نباشد، باید مراحل گفته شده در این سند را برای سایت مورد نظر خود انجام دهید.

۳ ایجاد درخواست امضای گواهی (CSR) و کلید خصوصی

برای دریافت گواهی الکترونیکی از مرکز صدور گواهی الکترونیکی پارس‌ساین، ابتدا باید یک درخواست امضای گواهی[1] (CSR) ایجاد نماییم. لازم به ذکر است که فیلدهای CSR باید طبق سیاست‌های مرکز صدور گواهی پارس‌ساین تکمیل گردد. در غیر این صورت، مرکز پارس‌ساین برای آن CSR، گواهی الکترونیکی صادر نخواهد کرد.

در نرم‌افزار IIS، فرایند ایجاد CSR و تکمیل فیلدهای آن با «سند جامع پروفایل‌های زیرساخت کلید عمومی کشور» تطابق ندارد. از این‌رو توصیه می‌شود برای ایجاد CSR از نرم‌افزار ParsKey Utility متعلق به شرکت امن‌افزار گستر شریف استفاده نمایید. برای دریافت این نرم‌افزار به بخش دانلود سایت مرکز صدور گواهی الکترونیکی پارس‌ساین به آدرس http://www.parssignca.ir/ مراجعه کنید. همچنین، سند "راهنمای ایجاد CSR با استفاده از نرم‌افزار Parskey Utility" در بخش راهنماها از سایت مذکور قابل دانلود است. نحوه ایجاد CSR برای گواهی SSL، در بخش "پروفایل گواهی SSL" از سند مذکور تشریح شده است.

پس از ایجاد CSR و کلید خصوصی (این کلید هنگام ایجاد CSR تولید می‌گردد)، فایل CSR باید به مرکز صدور گواهی الکترونیکی پارس‌ساین تحویل داده شود تا گواهی SSL متناظر آن را صادر نماید. دقت نمایید برای صدور گواهی توسط مرکز پارس‌ساین، تنها به فایل CSR نیاز می‌باشد و نباید فایل کلید خصوصی به این مرکز تحویل داده شود.

هشدار: سرور از فایل کلید خصوصی برای رمزگذاری و رمزگشایی داده‌ها استفاده می‌نماید. از این‌رو، در محافظت از کلید خصوصی دقت نمایید. در صورتی که این کلید در دسترس افراد غیرمجاز قرار گیرد، کلیه داده‌های رمزشده بین وب‌سایت و کاربران می‌تواند توسط این افراد رمزگشایی شود.

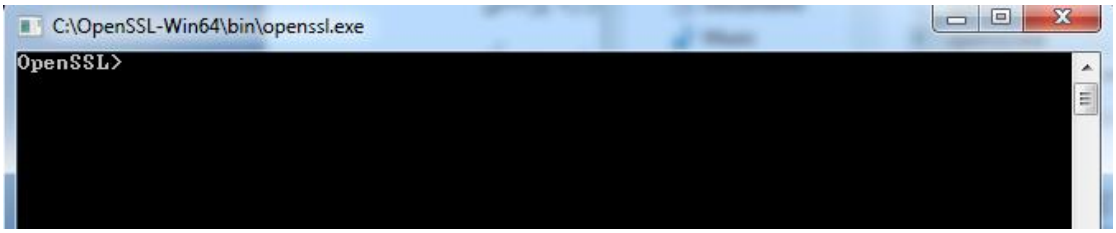
۴ ایجاد فایل گواهی به فرمت PFX

پس از دریافت گواهی الکترونیکی SSL از مرکز پارس‌ساین، باید آن را به فایلی با فرمت PFX تبدیل نماییم که شامل گواهی SSL صادرشده و کلید خصوصی متناظر آن می‌باشد. ابتدا باید از PEM بودن

[1] Certificate Signing Request (CSR)

فرمت فایل‌های گواهی و فایل کلید خصوصی اطمینان حاصل نماییم. لازم به ذکر است، در صورتی که CSR با نرم‌افزار ParsKey Utility تولید شده باشد، فایل کلید خصوصی در فرمت PEM می‌باشد. نحوه بررسی PEM بودن فایل کلید خصوصی در بخش ۸-۱ از پیوست تشریح شده است. همچنین، نحوه بررسی PEM بودن فایل گواهی، در بخش ۸-۲ از پیوست آمده است. برای ایجاد این فایل مراحل زیر را انجام می‌دهیم:

۱. نرم‌افزار OpenSSL را از بخش دانلود وب‌سایت مرکز صدور گواهی الکترونیکی پارس‌ساین به آدرس www.parssignca.ir دریافت و روی سیستم خود نصب می‌نماییم.
۲. اگر نسخه‌ی تحت ویندوز OpenSSL را نصب کرده باشیم، به دایرکتوری bin در مسیر نصب نرم‌افزار رفته (این مسیر در ویندوز 7 نسخه ۶۴ بیتی، C:\OpenSSL-Win64\bin می‌باشد) و فایل اجرایی OpenSSL به نام openssl.exe را اجرا می‌نماییم. با اجرای این برنامه، پنجره‌ای مانند شکل زیر ظاهر می‌گردد.



۳. روبروی عبارت <OpenSSL در پنجره فوق، دستور زیر را وارد می‌نماییم:

```
pkcs12 -export -out mydomain.pfx -inkey key.pem -in mydomain.cer
```

لازم به ذکر است که اگر با لینوکس کار می‌کنیم، فرمان زیر را به جای دستور فوق باید وارد نماییم:

```
openssl pkcs12 -export -out mydomain.pfx -inkey key.pem -in
mydomain.cer
```

در دستور فوق:

- key.pem، فایل کلید خصوصی با فرمت PEM می‌باشد؛
- mydomain.cer، فایل گواهی با فرمت PEM می‌باشد؛
- mydomain.pfx، فایل خروجی ایجاد شده با فرمت PEM می‌باشد.

با وارد نمودن دستور فوق، از ما خواسته می‌شود گذرواژه کلید خصوصی (که هنگام ایجاد CSR تعیین نموده‌ایم) را وارد نماییم. در مرحله بعد، از ما خواسته می‌شود گذرواژه فایل PFX را وارد نماییم، که باید گذرواژه‌ای را وارد نماییم تا فایل PFX ایجاد گردد. دقت کنید، هنگام تایپ این گذرواژه‌ها، کاراکترهای

آن‌ها در صفحه نمایش داده نمی‌شود و مکان‌نما حرکت نمی‌کند؛ شما بدون توجه به این مسأله گذرواژه را وارد کنید). گذرواژه را به خاطر بسپارید زیرا هنگام نصب گواهی باید آن را وارد نمایید.

لازم به ذکر است در دستور فوق، باید برای هر یک از فایل‌ها، مسیر دقیق آن‌ها را وارد نماییم. برای مثال، در صورتی که فایل‌های key.pem و mydomain.cer، و را در پوشه‌ی certs از درایو D قرار داده باشیم و بخواهیم فایل mydomain.pfx نیز در همین مسیر ذخیره گردد، دستور به صورت زیر خواهد بود:

```
pkcs12 -export -out d:\certs\mydomain.pfx -inkey d:\certs\key.pem
-in d:\certs\mydomain.cer
```

در صورت استفاده از لینوکس، فرض می‌کنیم فایل‌های مذکور در مسیر home/certs/ قرار داشته باشند. به این ترتیب، دستور به صورت زیر خواهد بود:

```
openssl pkcs12 -export -out /home/certs/mydomain.pfx -inkey
/home/certs/key.pem -in /home/certs/mydomain.cer
```

۵ پیکربندی IIS به منظور استفاده از گواهی الکترونیکی

پس از ایجاد فایل PFX گواهی SSL (طبق بخش ۴)، می‌توانیم تنظیمات لازم را در نرم‌افزار IIS 7 به ترتیب زیر انجام دهیم:

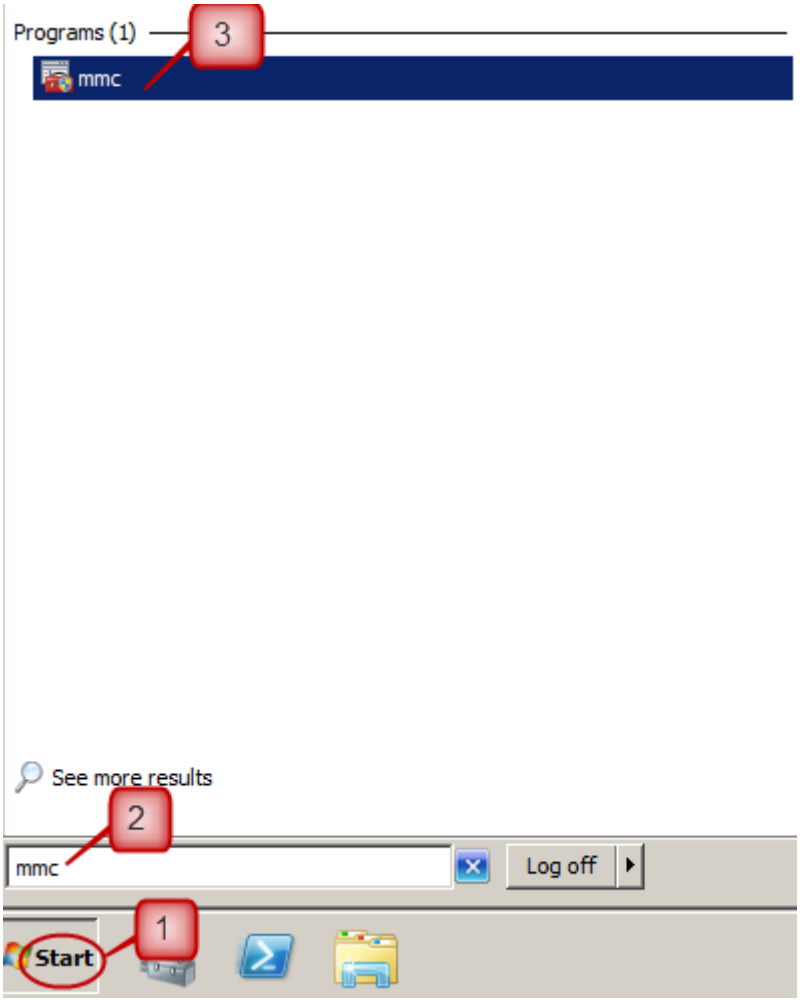
۱. **نصب گواهی الکترونیکی به فرمت PFX روی سرور؛**
۲. **تخصیص گواهی به وب‌سایت مورد نظر در IIS؛**
۳. **تنظیم وب‌سرور برای اجباری نمودن استفاده از پروتکل HTTPS.**

در بخش‌های بعد، هر یک از مراحل فوق با جزییات تشریح می‌گردد.

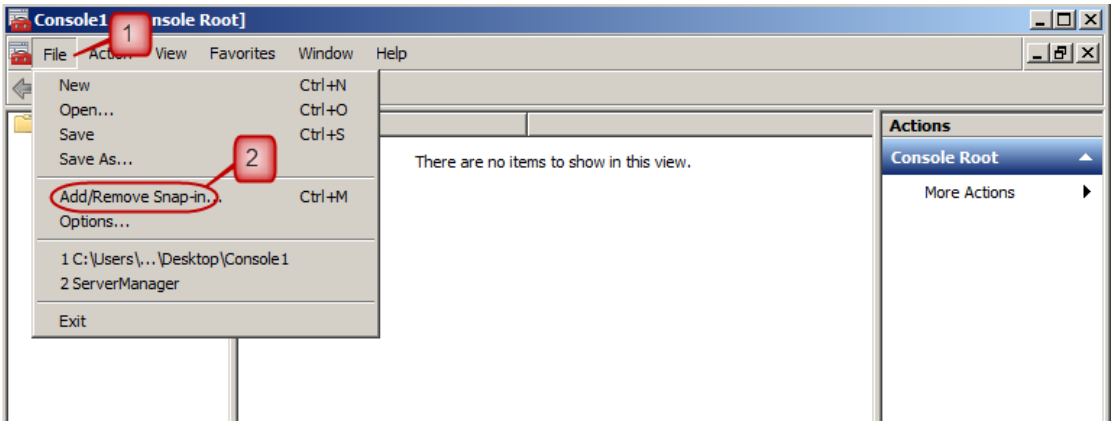
۱-۵ نصب گواهی الکترونیکی روی سرور

پس از ایجاد فایل گواهی به فرمت PFX مطابق بخش ۴، فایل گواهی PFX را روی سروری که برای آن گواهی SSL صادر شده است، نصب می‌نماییم. رویه این کار به صورت زیر می‌باشد:

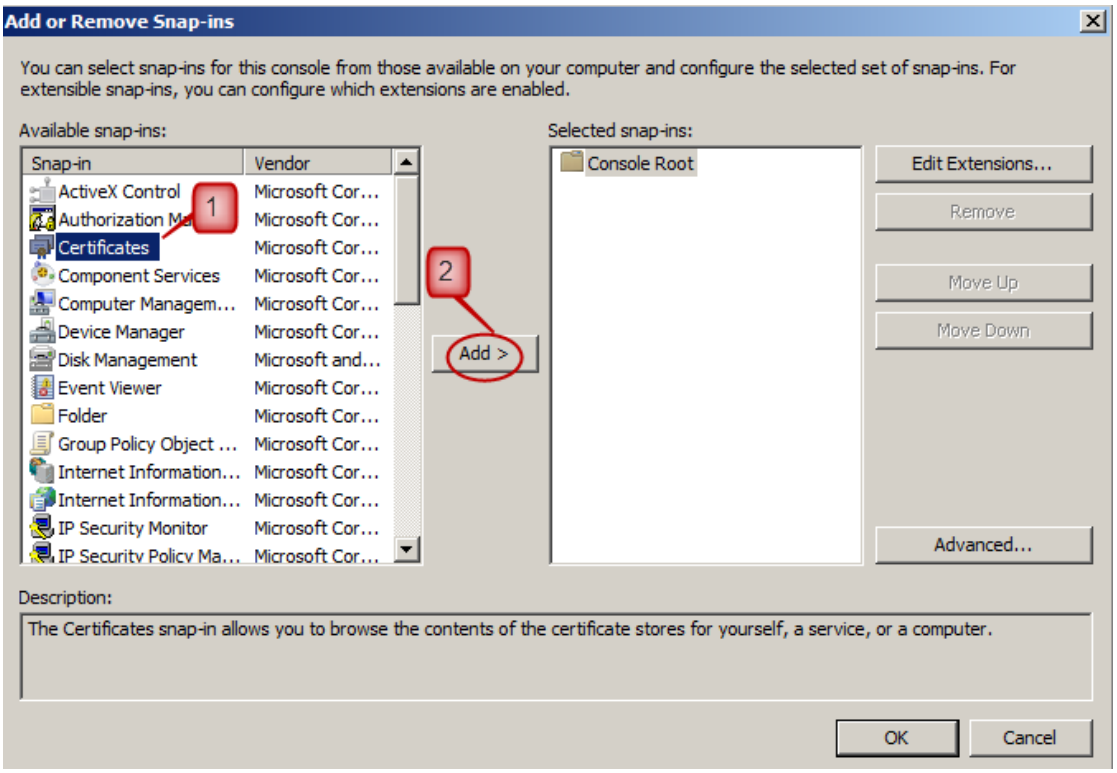
۱. در منوی Start، عبارت mmc را در جعبه search programs and files وارد می‌نماییم تا برنامه mmc در لیست Programs ظاهر گردد، روی آن کلیک می‌کنیم (شکل زیر).



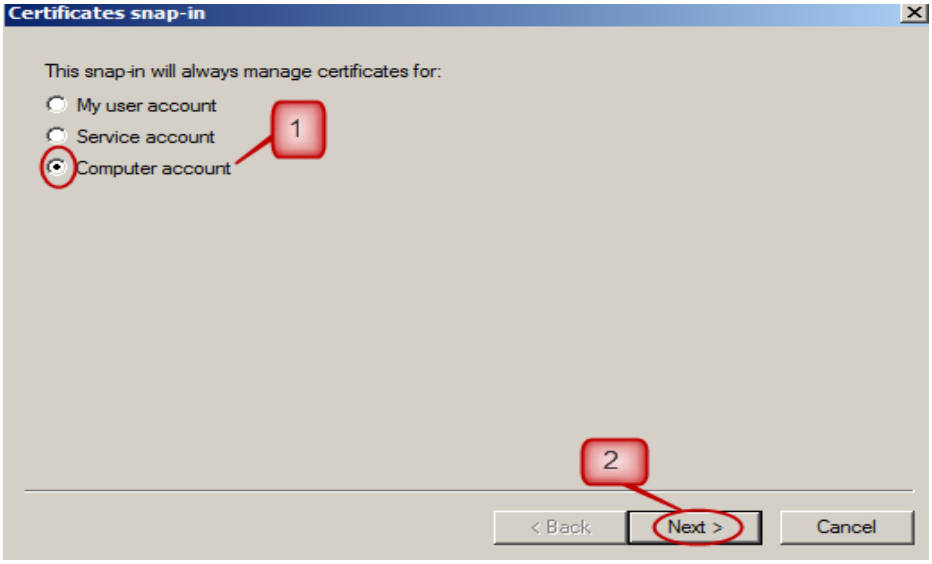
۲. در کنسول بازشده، در سربرگ File روی گزینه Add/Remove Snap-in کلیک می‌نماییم (شکل زیر).



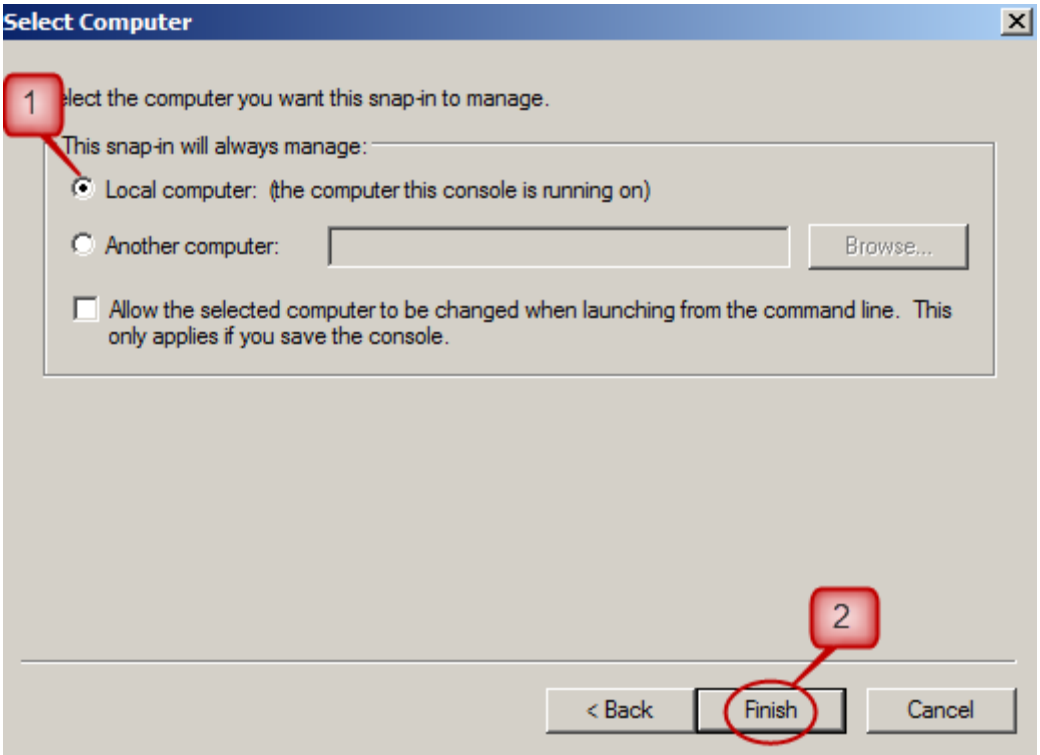
۳. در پنجره Add or Remove Snap-ins، گزینه Certificates را انتخاب نموده (مرحله ۱ از شکل زیر) و سپس روی Add کلیک می‌نماییم (مرحله ۲ از شکل زیر).



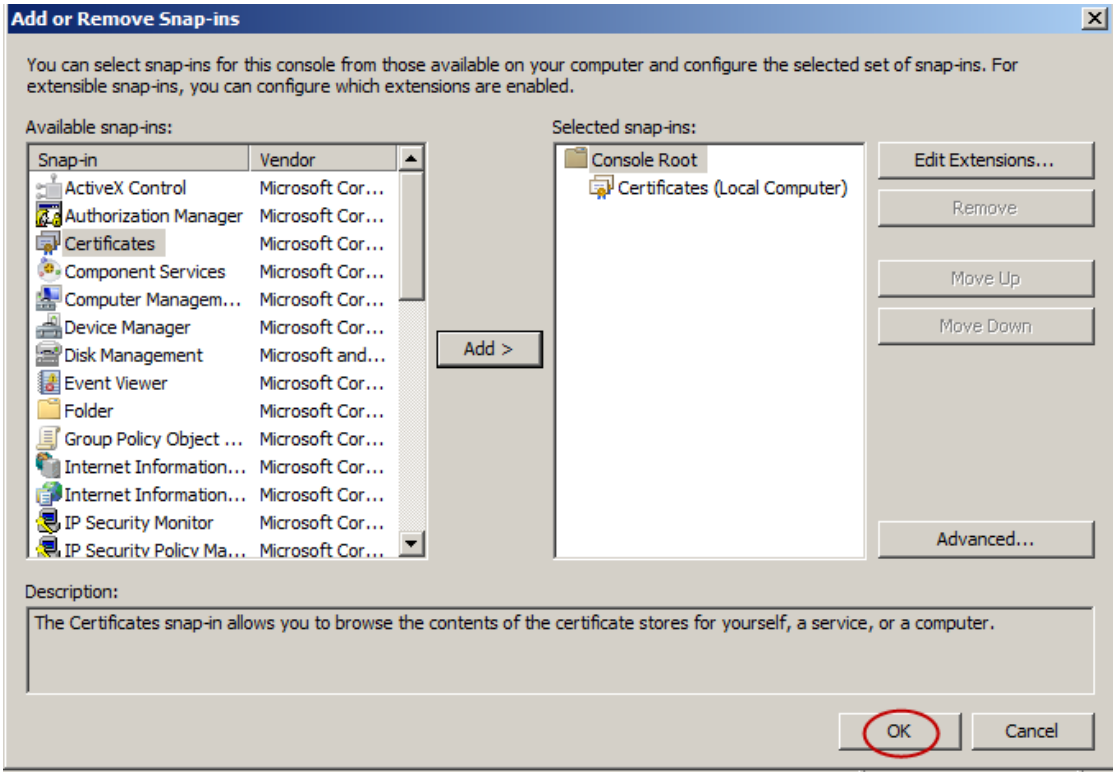
۴. در پنجره Certificates snap-in، گزینه Computer account را انتخاب نموده و روی Next کلیک می‌نماییم (شکل زیر).



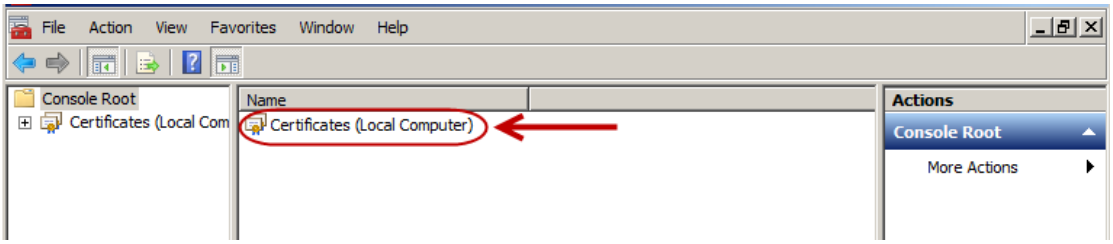
۵. در پنجره Select Computer، گزینه Local computer به صورت پیش‌فرض انتخاب شده می‌باشد. بدون تغییر آن روی Finish کلیک می‌نماییم (شکل زیر).



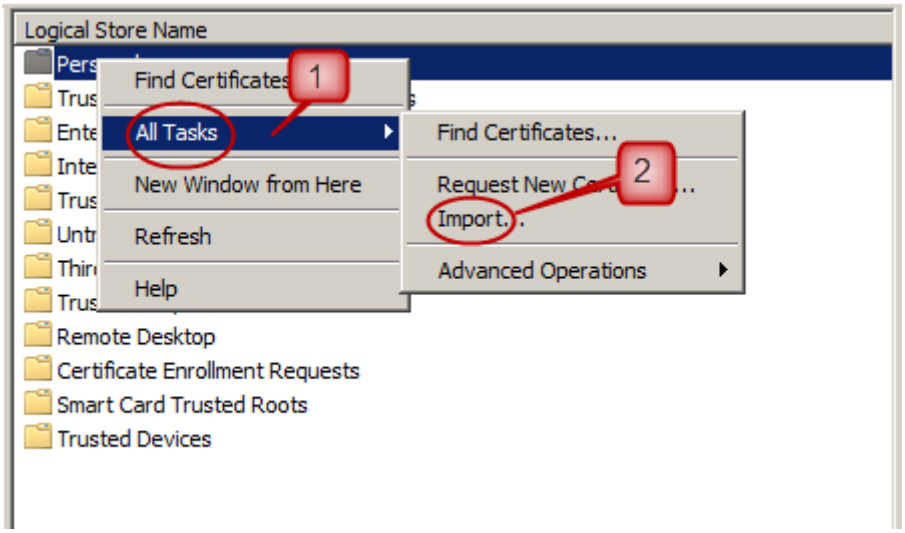
۶. در پنجره Add or Remove Snap-ins، روی OK کلیک می‌نماییم (شکل زیر).



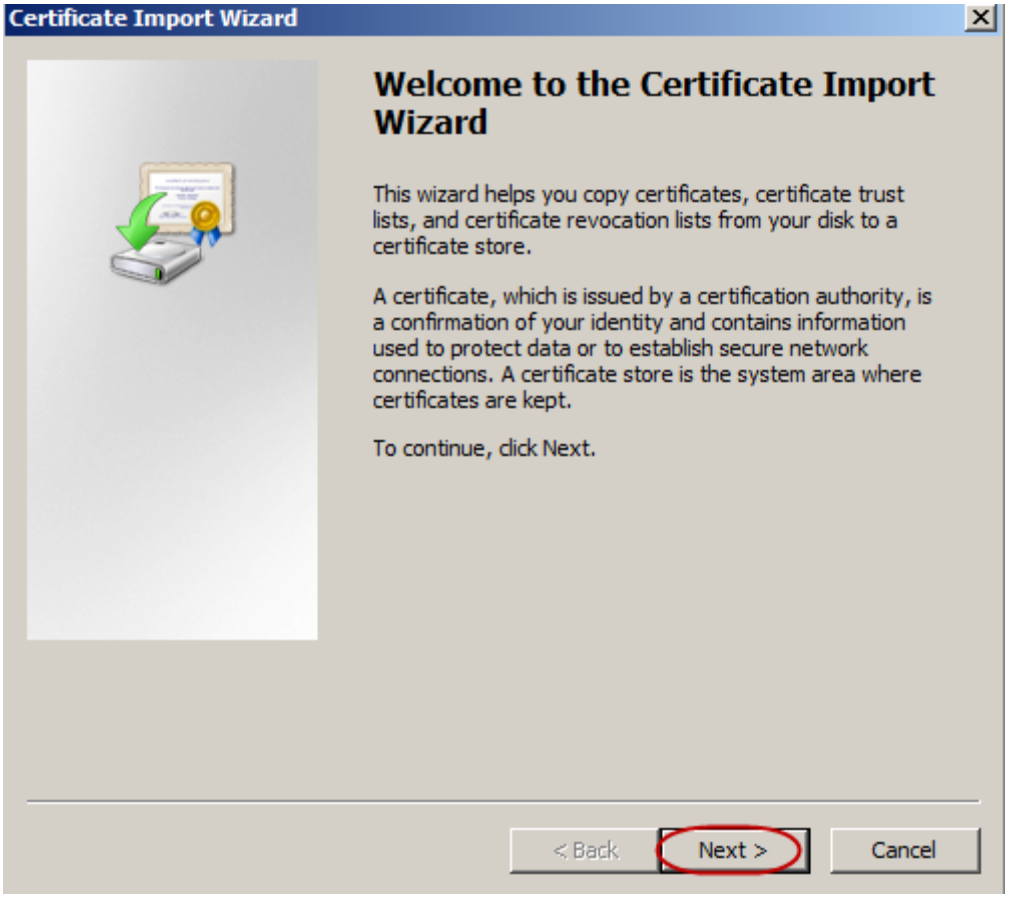
۷. در منوی وسط، روی Certificates (Local Computer) دو بار کلیک می‌نماییم (شکل زیر).



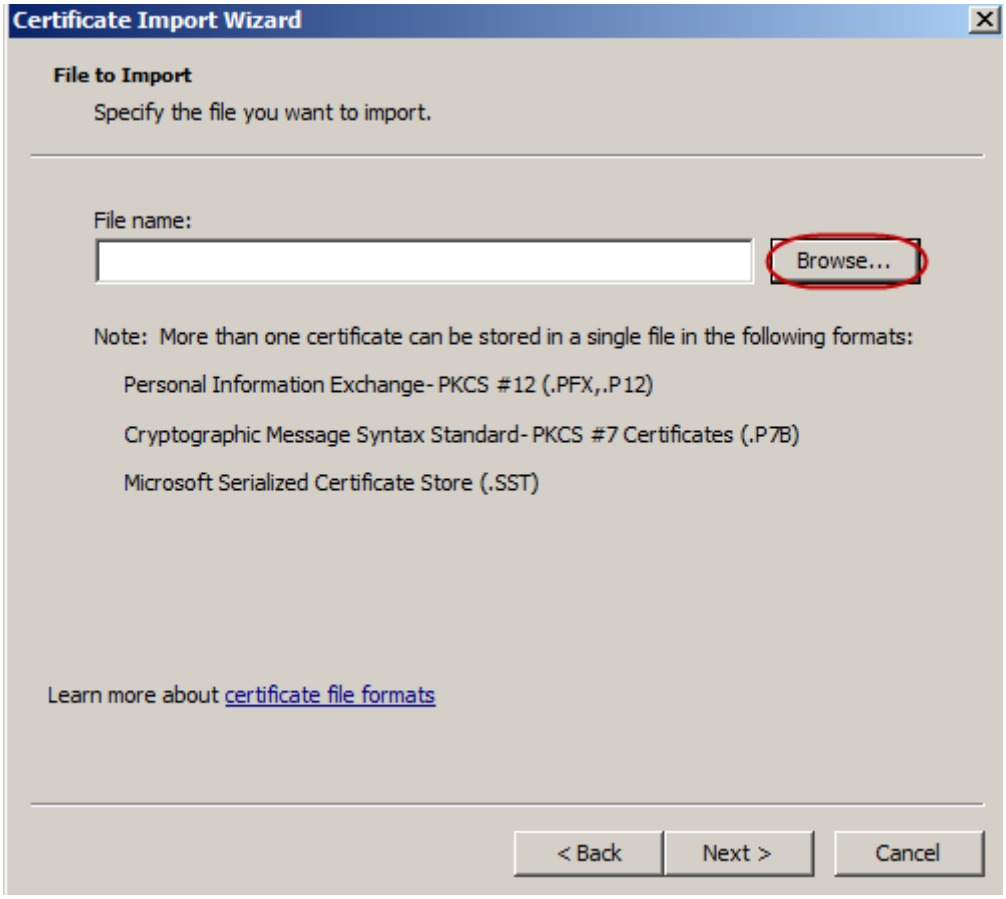
۸. در بخش Logical Store Name، روی Personal کلیک راست نموده، گزینه All Tasks (مرحله ۱ از شکل زیر) و سپس Import را انتخاب می‌نماییم (مرحله ۲ از شکل زیر).



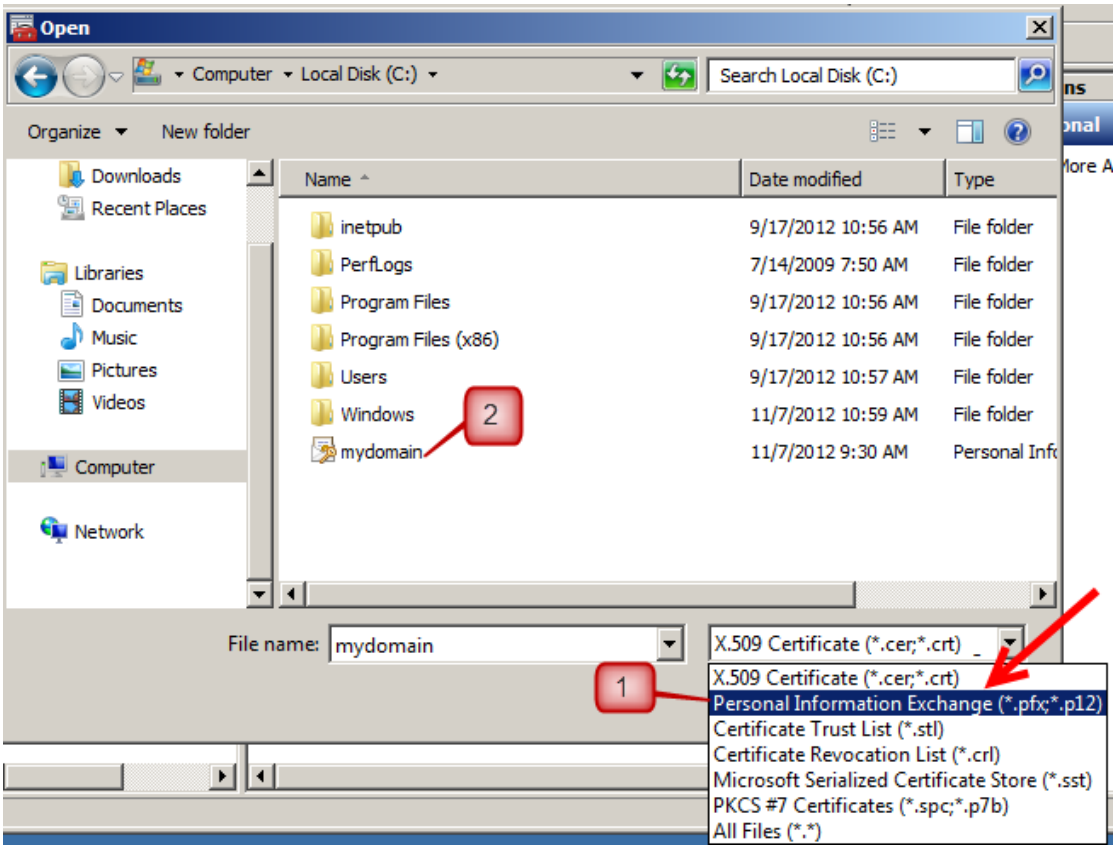
۹. در پنجره Certificate Import Wizard، روی Next کلیک می‌نماییم (شکل زیر).



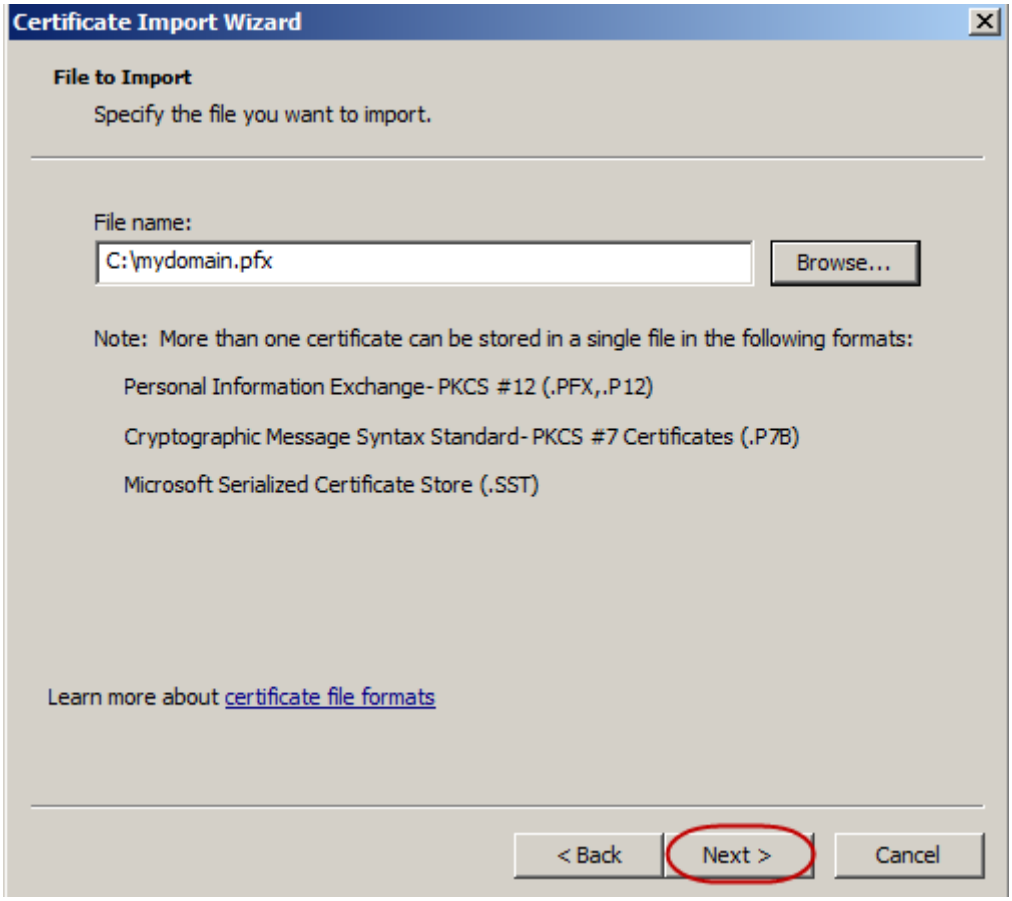
۱۰. با کلیک روی Browse، فایل گواهی با فرمت PFX را انتخاب نموده و سپس روی Next کلیک می‌نماییم.



۱۱. فرمت فایل را از نوع Personal Information Exchange (*.pfx;*.p12) قرار داده (مرحله ۱ از شکل زیر)، سپس فایل pfx را در مسیر ذخیره آن انتخاب نموده (مرحله ۲ از شکل زیر) و روی دکمه Open کلیک می‌نماییم.

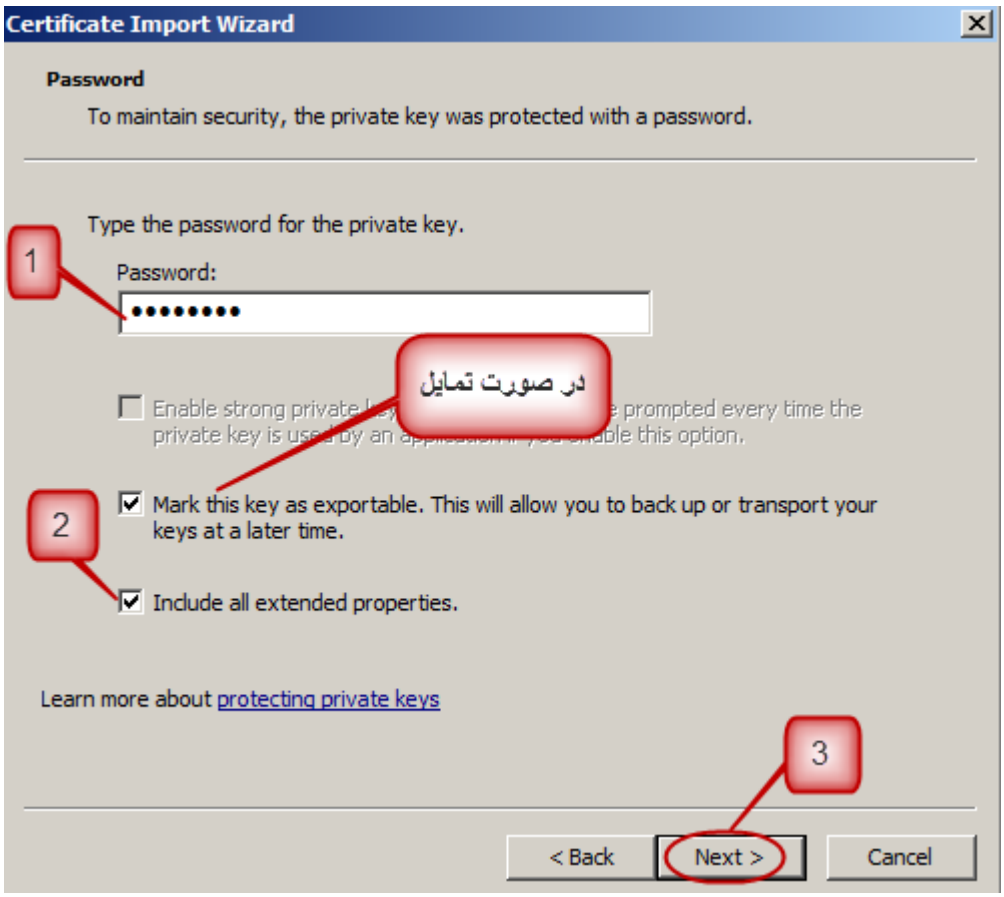


۱۲. پس از وارد نمودن فایل گواهی با فرمت PFX، روی Next کلیک می‌نماییم (شکل زیر).

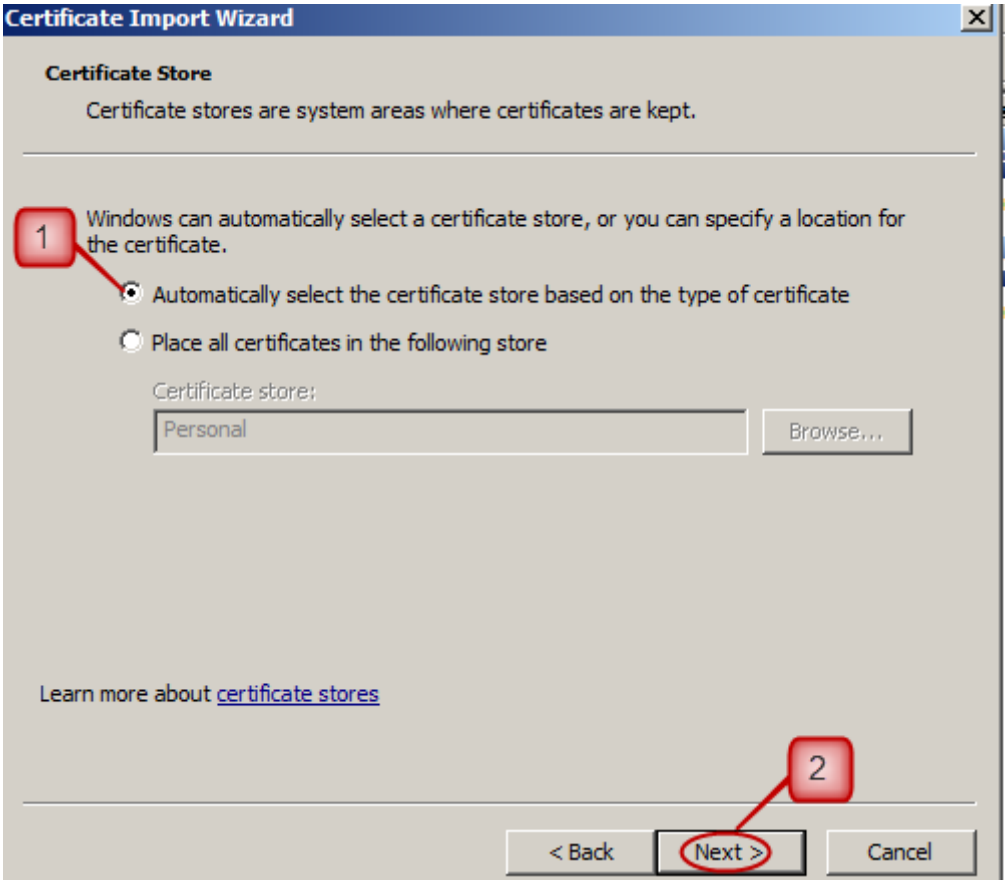


۱۳. گذرواژه‌ای که هنگام ایجاد فایل pfx تعیین نموده‌ایم را وارد می‌نماییم (مرحله ۱ از شکل زیر). در صورت تمایل، می‌توانید گزینه "Mark this key as exportable..." را انتخاب نمایید. گزینه "Include all extended properties" به صورت پیش‌فرض انتخاب شده است (مرحله ۲ از شکل زیر)، بدون تغییر آن روی Next کلیک می‌نماییم (مرحله ۳ از شکل زیر).

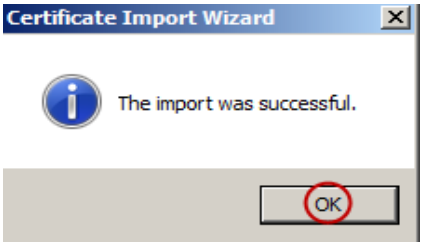
نکته: با انتخاب گزینه "Mark this key as exportable..."، به منظور انتقال فایل pfx به سرور دیگر یا تهیه نسخه پشتیبان از آن، می‌توانیم فایل pfx را استخراج نماییم. در صورتی که به دلیل حساسیت امنیتی نخواهید کلید خصوصی از روی سرور قابل استخراج باشد، این گزینه را انتخاب نکنید (آن را تیک نزنید).



۱۴. گزینه "Automatically select the certificate store based on the type of certificate" را انتخاب نموده و روی Next کلیک می‌نماییم (شکل زیر).



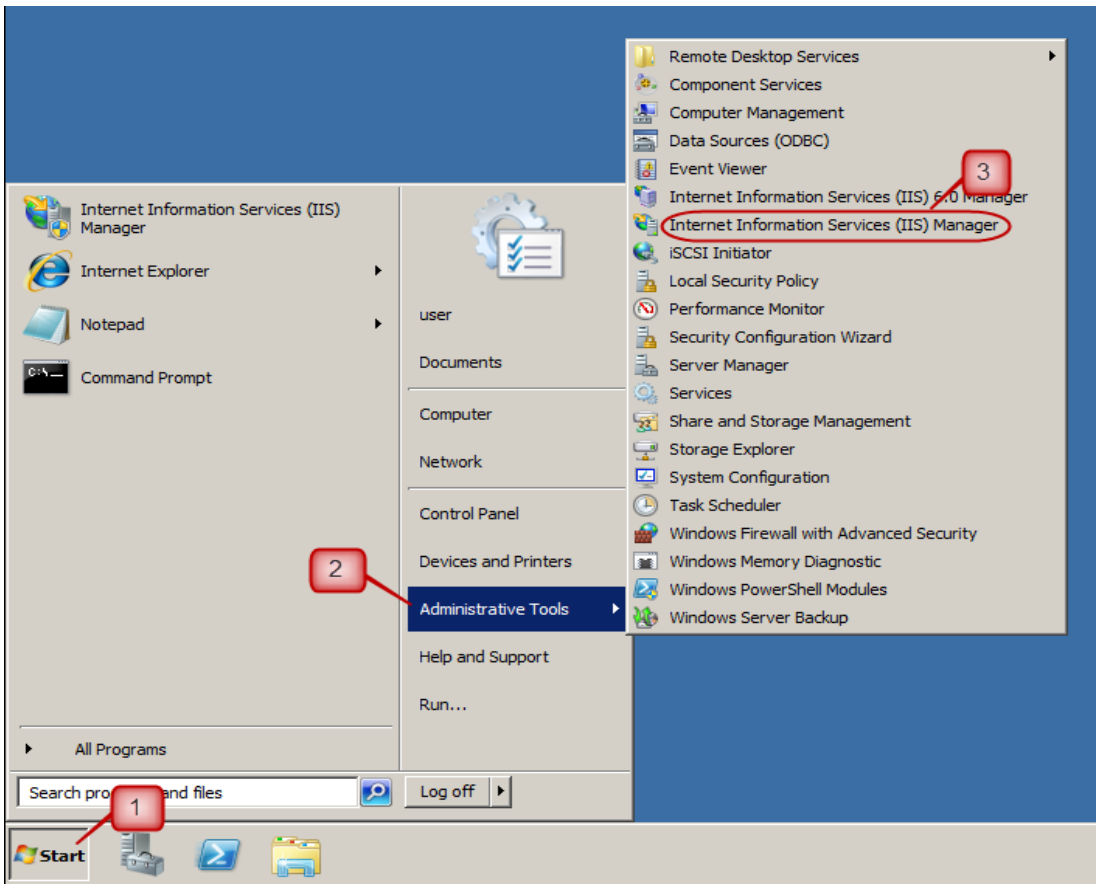
۱۵. پیغامی مبنی بر موفق بودن نصب گواهی ظاهر می‌گردد. روی OK کلیک می‌نماییم (شکل زیر). در پایان پنجره کنسول را می‌بندیم. لازم به ذکر است نیازی به ذخیره کردن کنسول نمی‌باشد.



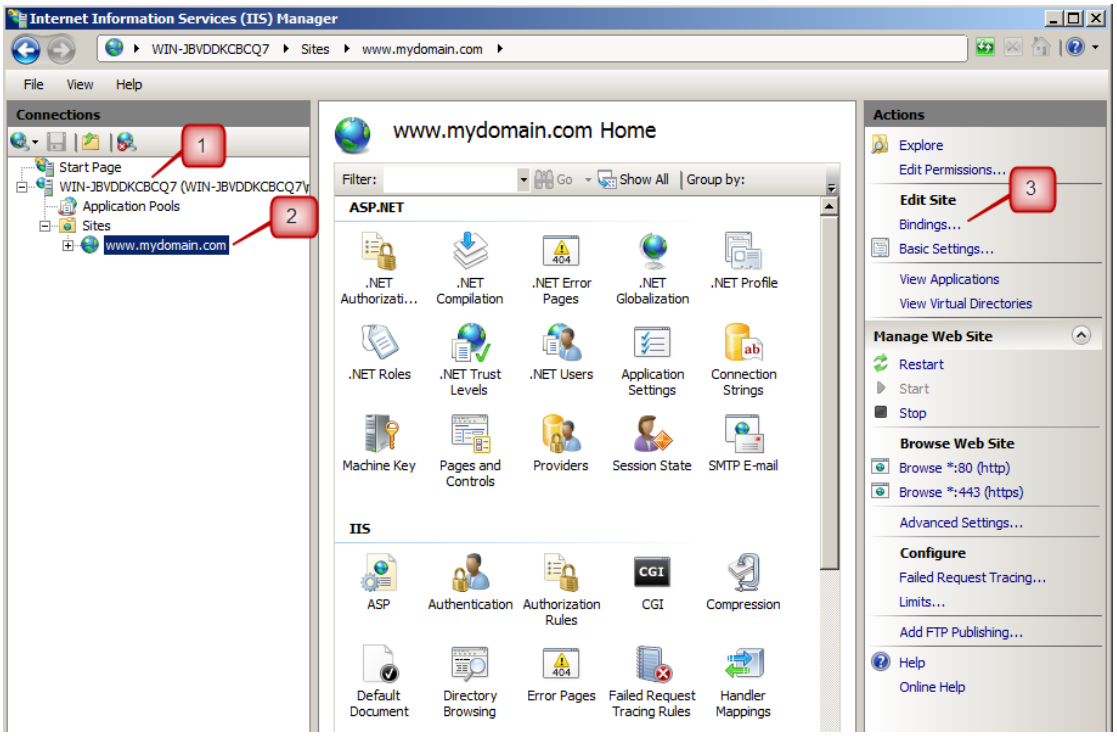
۲-۵ تخصیص گواهی به وب‌سایت

پس از نصب گواهی روی سرور، باید در نرم‌افزار IIS آن را به وب‌سایت مورد نظر تخصیص دهیم. رویه این کار به صورت زیر می‌باشد:

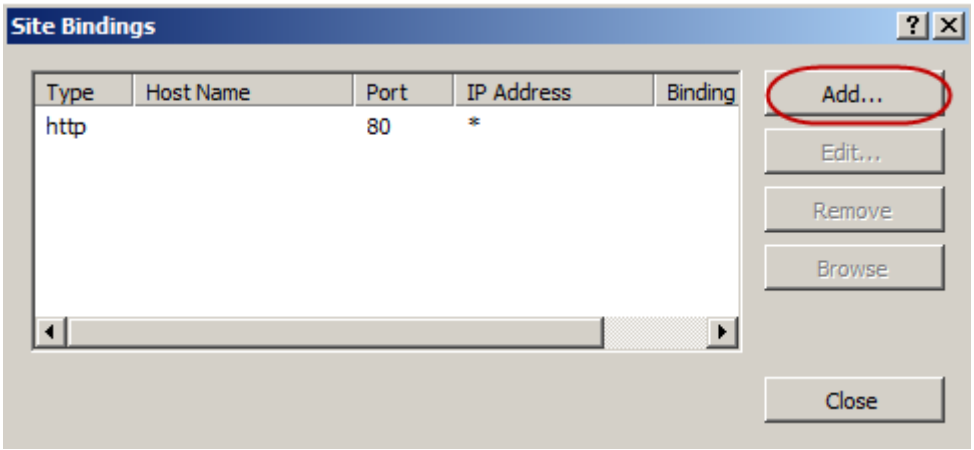
۱. در منوی Start، در بخش Administrative Tools، روی Internet Information Services (IIS) Manager کلیک می‌نماییم (شکل زیر).



۲. در منوی Connections روی نام سرور مورد نظر کلیک می‌نماییم (مرحله ۱ از شکل زیر). در لیست Sites، سایت مورد نظر را انتخاب می‌کنیم (در مرحله ۲ از شکل زیر). در منوی Actions، روی گزینه Bindings کلیک می‌نماییم (مرحله ۳ از شکل زیر).



۳. در پنجره بازشده (شکل زیر)، روی دکمه Add کلیک می‌نماییم.



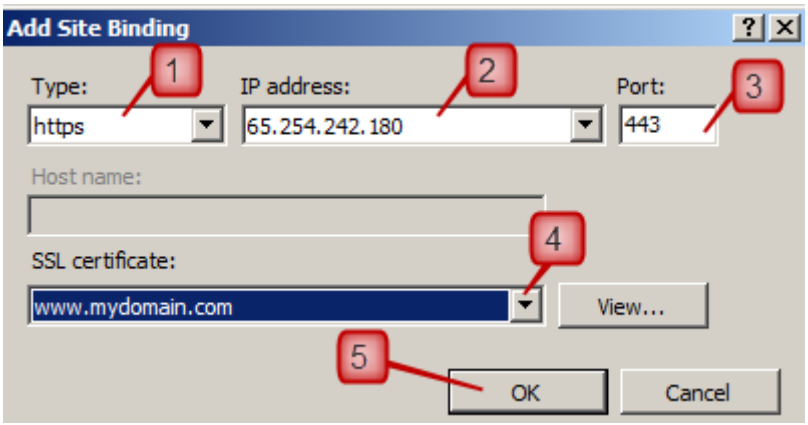
۴. در پنجره بازشده (شکل زیر)، تنظیمات زیر را انجام می‌دهیم:

- از لیست Type، گزینه HTTPS را انتخاب می‌کنیم (مرحله ۱ از شکل زیر).
- از لیست IP Address، آدرس IP سایت را را انتخاب می‌کنیم (مرحله ۲ از شکل زیر).

نکته بسیار مهم: برای استفاده از HTTPS برای یک دامنه (وب‌سایت)، باید یک آدرس IP اختصاصی[1] به آن دامنه تخصیص دهیم. این آدرس نباید با دامنه‌های دیگر به اشتراک گذاشته شود. در غیر این‌صورت، امکان استفاده از HTTPS وجود نخواهد داشت.

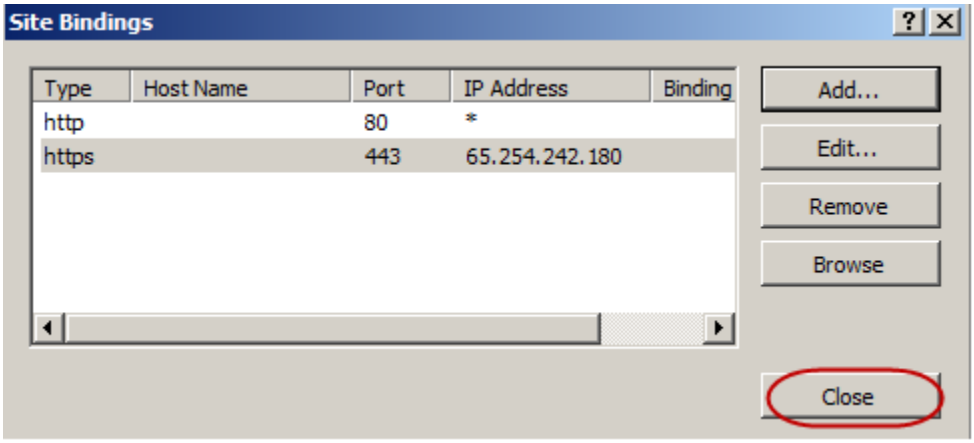
- از لیست Port، شماره درگاه 443 (شماره درگاه پیش‌فرض) را انتخاب می‌کنیم (مرحله ۳ از شکل زیر). در صورت تمایل، می‌توانیم شماره درگاه دیگری را نیز وارد کنیم. در این صورت، دسترسی به سایت از طریق HTTPS باید با استفاده از این شماره درگاه انجام شود. از این‌رو، کاربران وب‌سایت باید از این شماره درگاه مطلع شوند.
- از لیست SSL Certificate، گواهی مربوط به وب‌سایت را مطابق مرحله ۴ از شکل زیر انتخاب می‌کنیم (این گواهی قبلاً طبق بخش ۵-۱ روی سرور نصب شده است).

در پایان، روی دکمه OK کلیک می‌نماییم (شکل زیر).



[1] Dedicated IP Address

۵. در پنجره زیر، روی دکمه Close کلیک می‌نماییم.



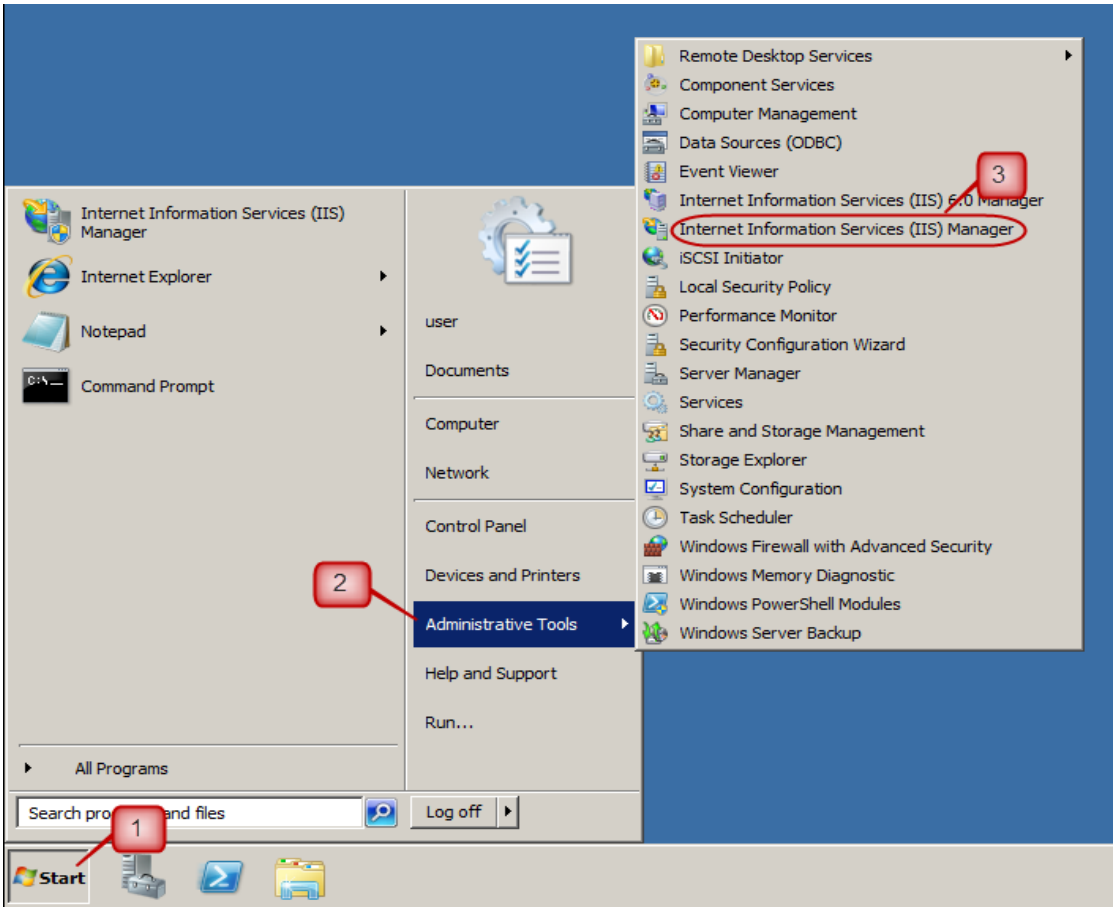
پس از این مرحله، گواهی HTTPS به وب‌سایت تخصیص داده شده است و با استفاده از HTTPS می‌توان به سایت دسترسی داشت با این وجود، در برخی موارد باید IIS راه‌اندازی مجدد[1] شود تا بتوان از سرویس HTTPS استفاده نمود. لازم به ذکر است که در این مرحله با استفاده از HTTP نیز می‌توان به سایت دسترسی داشت؛ به منظور برقراری ارتباط تنها از طریق HTTPS، باید طبق بخش ۵-۳ عمل نماییم.

[1] Restart

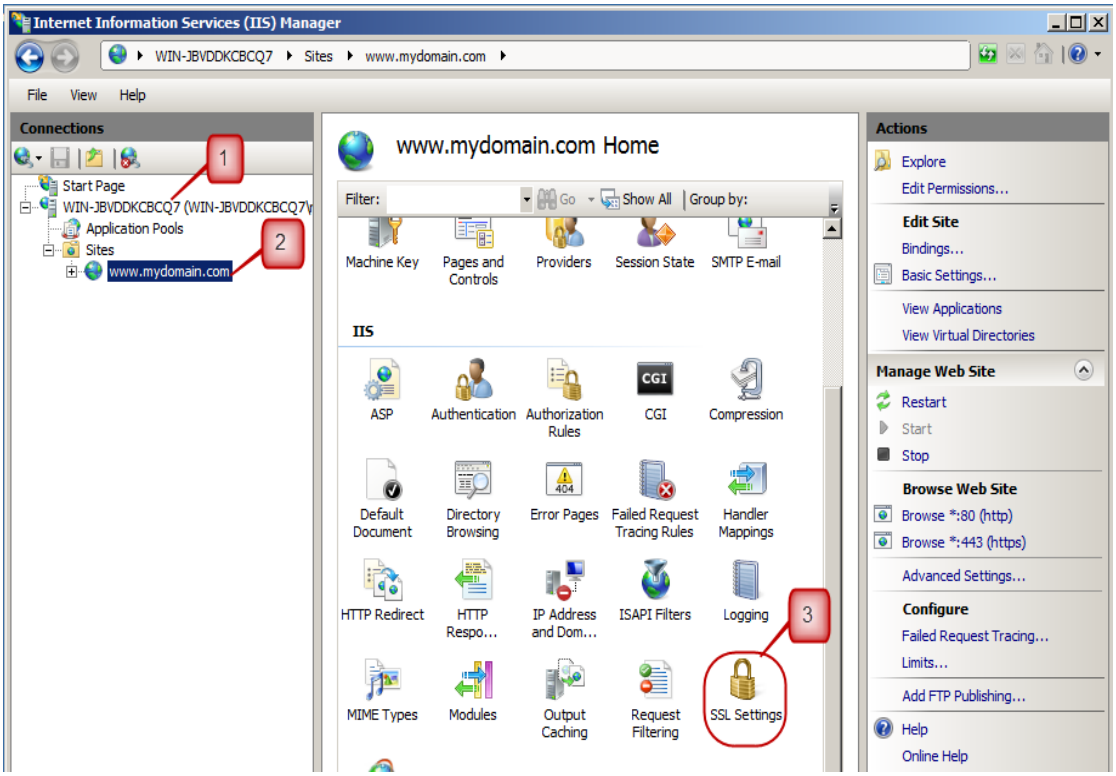
۳-۵ اجباری کردن اتصال HTTPS

برای آن‌که اتصال به سایت مورد نظر تنها به صورت HTTPS قابل انجام باشد، باید تنظیمات لازم در نرم‌افزار IIS انجام شود. در غیر این صورت، کاربران در صورت تمایل می‌توانند با پروتکل ناامن HTTP به سایت متصل شوند و در نتیجه در معرض مخاطرات امنیتی مختلفی قرار گیرند. برای اجباری نمودن برقراری ارتباط HTTPS به سایت، به صورت زیر عمل می‌نماییم:

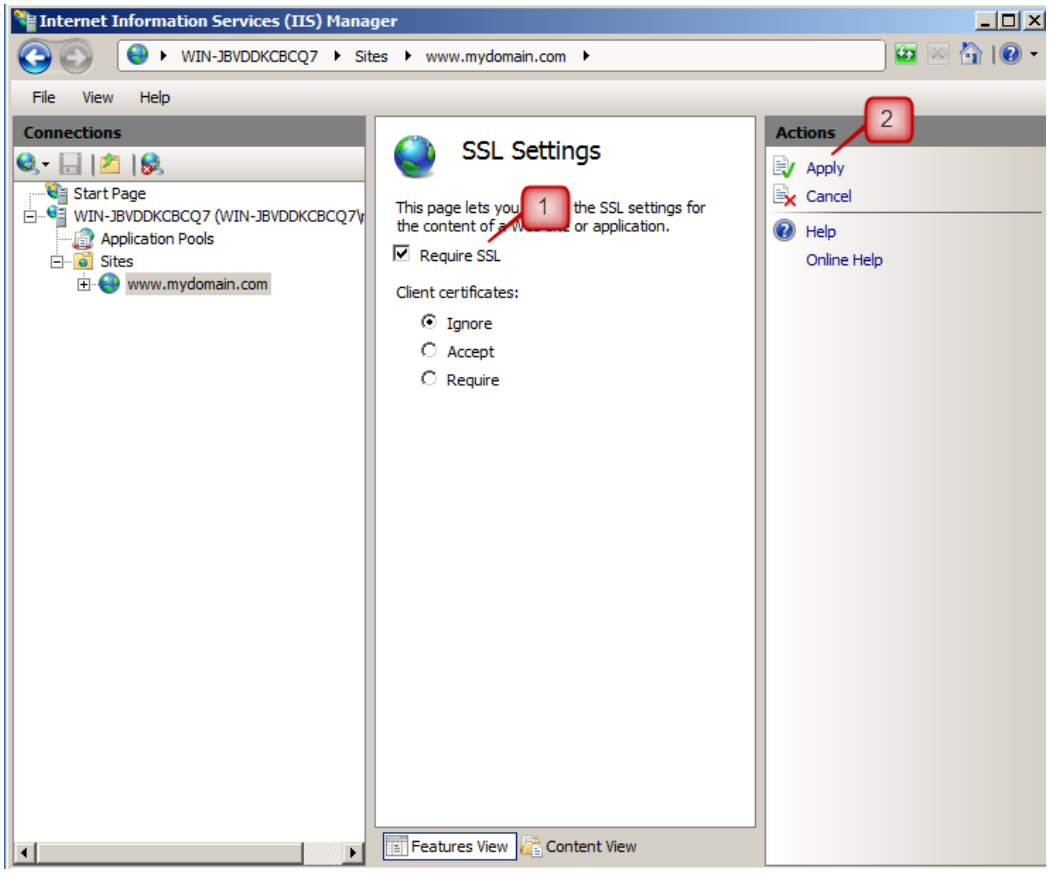
۱. در منوی Start، در بخش Administrative Tools روی Internet Information Services (IIS) Manager کلیک می‌نماییم (شکل زیر).



۲. در منوی Connections روی نام سرور مورد نظر کلیک می‌نماییم (مرحله ۱ از شکل زیر). در لیست Sites، سایت مورد نظر را انتخاب می‌کنیم (مرحله ۲ از شکل زیر). در منوی وسط روی SSL Settings دابل‌کلیک می‌نماییم (مرحله ۳ از شکل زیر).



۳. در پنجره بازشده (شکل زیر)، گزینه Require SSL را انتخاب می‌کنیم (مرحله ۱ از شکل زیر). در بخش Client certificates نیز می‌توانیم بسته به سیاست‌های وب‌سایت خود در دسترسی سرویس‌گیرندگان، گزینه مناسب را انتخاب نماییم؛ گزینه پیش‌فرض، گزینه Ignore می‌باشد. در پایان، در منوی Actions روی Apply کلیک می‌نماییم (مرحله ۲ از شکل زیر). در صورت موفق‌بودن اِعمال تغییرات، در منوی Actions عبارت The changes have been successfully applied نمایش داده می‌شود.



۶ بررسی صحت نصب گواهی SSL

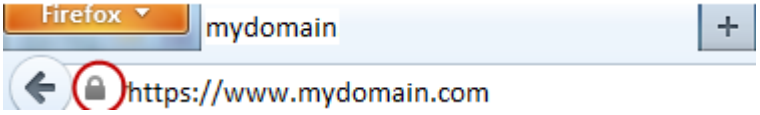
برای برقراری ارتباط صحیح SSL میان مرورگر کاربر و وب‌سایت، کاربر وب‌سایت باید زنجیره گواهی را روی سیستم یا مرورگر خود نصب نماید. رویه این کار در سند «راهنمای نصب زنجیره گواهی» تشریح شده است. این سند را می‌توانید از بخش "راهنماها" در وب‌سایت مرکز پارس‌ساین به آدرس www.parssignca.ir دانلود و مطالعه نمایید. پس از نصب صحیح زنجیره گواهی، در نوار آدرس مرورگر، آدرس https://www.mydomain.com را وارد می‌نماییم (به جای www.mydomain.com باید آدرس

دقیق سایت خود را وارد نمایید). نمایش علامت قفل به همراه عبارت https در نوار آدرس مرورگرها یکی از نشانه‌های صحیح بودن نصب گواهی SSL در وب‌سایت می‌باشد. نمایش علامت قفل در سه مرورگر Google Chrome، Internet Explorer، و Firefox به صورت زیر می‌باشد:

- **مرورگر Google Chrome**: در نوار آدرس (مطابق شکل زیر) قفل سبز رنگ در کنار عبارت سبز رنگ https ظاهر می‌شود.

- **مرورگر Internet Explorer**: علامت قفل در سمت راست نوار آدرس (شکل زیر) ظاهر می‌شود.

- **مرورگر فایرفاکس**: در نوار آدرس (مطابق شکل زیر) آیکن قفل کنار عبارت https ظاهر می‌شود.



برای اطمینان کامل از صحت نصب گواهی، در مرورگر خود روی علامت قفل کلیک نموده و روی لینک Certificate Information در Google Chrome، View Certificates در Internet Explorer، و More Information در Firefox کلیک نمایید. سپس اطمینان حاصل کنید که گواهی نشان‌داده شده، همان گواهی است که مرکز پارس‌ساین برای وب‌سایت شما صادر نموده است.

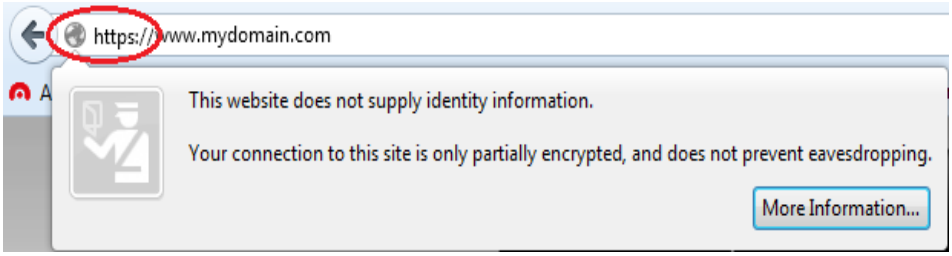
۷ مشکلات احتمالی پس از نصب گواهی

۷-۱ عدم نمایش قفل کنار عبارت https و عدم نمایش صحیح وب‌سایت

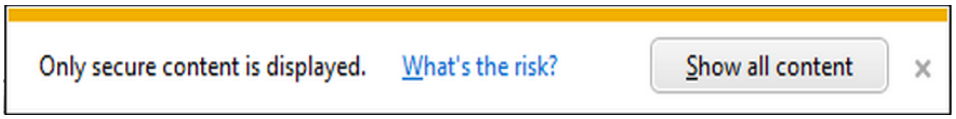
در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکل‌های زیر نمایش داده شود:

- **مرورگر Google Chrome**: در نوار آدرس مرورگر، علامت مثلث روی قفل کنار https نشان داده شود (مانند شکل زیر).

- **مرورگر Firefox**: در نوار آدرس مرورگر، علامت قفل کنار https ظاهر نشود (مانند شکل زیر).



- **مرورگر Intenet Explorer**: در پایین صفحه، پیامی مانند شکل زیر ظاهر گردد.



- **مرورگر Opera**: در نوار آدرس مرورگر، علامت Secure کنار https ظاهر نشود (مانند شکل زیر).

- **مرورگر Safari**: در انتهای نوار آدرس مرورگر، علامت قفل ظاهر نشود (مانند شکل زیر).

این مشکل معمولاً Mixed content warning نامیده می‌شود که ممکن است یک حمله‌کننده با استفاده از آن امنیت کاربران سایت شما را به مخاطره اندازد. این مشکل مربوط به گواهی SSL

سایت نیست، بلکه به کد وب‌سایت یا تنظیمات سرور شما مربوط می‌باشد. دلیل مشکل این دلیل است که در وب‌سایت شما از محتوای[1] ناامن استفاده شده است. مثال‌هایی از محتوای ناامن، عکس‌ها، اسکریپت‌ها، یا CSSهایی هستند که به طور ناامن (از طریق HTTP) در سایت شما بارگذاری می‌شوند. مرورگر از بارگذاری یا اجرای این محتواها جلوگیری می‌کند. به همین دلیل ممکن است CSS وب‌سایت شما بارگذاری نشده و ساختار وب‌سایت شما با HTTPS به هم بریزد، عکسی بارگذاری نشود، یا اسکریپتی اجرا نشود.

برای کشف محتوای ناامن، می‌توانید از قابلیت Web Developer Toolbar در اغلب مرورگرها استفاده کنید. کشف محتوای ناامن با استفاده از مرورگرهای رایج معمولاً به صورت زیر می‌باشد:

- **مرورگر Google Chrome و Internet Explorer**: فشردن کلید F12 و مشاهده خطاها در بخش Console.
- **مرورگر Firefox**: فشردن کلیدهای Ctrl + Shift + K و مشاهده خطاهای Mixed Content.

پس از کشف محتوای ناامن، آن‌ها را از طریق HTTPS بارگذاری نموده و در صورت عدم امکان بارگذاری با استفاده از HTTPS، آن‌ها را از وب‌سایت خود حذف نمایید. در زیر چند سناریو از محتوای ناامن توصیف شده است.

- برای مثال، فرض کنید CSS سایت به صورت http://www.mydomain.com/templates/mystyle.css در صفحه سایت فراخوانی شده باشد. در این صورت، به دلیل استفاده از http (به جای https) این محتوا توسط مرورگر ناامن تشخیص داده شده و بارگذاری نمی‌شود (در نتیجه ساختار سایت بهم می‌ریزد). بنابراین توصیه می‌شود به جای استفاده از آدرس‌های ثابت (hard-coded) برای عکس‌ها، CSS، و اسکریپت‌های سایت، از روش‌هایی مانند آدرس‌های نسبی، توابع (مثلاً ()include)، یا هر روش دیگری استفاده نمایید که با استفاده از آن بتوان محتوا را با استفاده از https بارگذاری نمود. در صورتی که از روشی مانند آدرس‌دهی نسبی استفاده کنید اما مشکل همچنان باقی باشد، مشکل مربوط به تنظیمات SSL در سرور شما می‌باشد.
- در برخی موارد، ممکن است آدرس عکس، CSS، یا اسکریپت با https باشد اما مرورگر آن را بارگذاری نکند. این مشکل معمولاً به این دلیل است که مثلاً CSS با آدرس

[1] Content

https://mydomain.com/templates/mycss.css (یعنی بدون www) فراخوانی شده است اما آدرس درج شده در گواهی سایت، با www است. در این مثال، راه حل این است آدرس https به طور دقیق و طبق آنچه در گواهی SSL سایت درج‌شده وارد شود.

- مثال دیگر از محتوای ناامن، استفاده از اسکریپت‌هایی است که با استفاده از http اطلاعاتی را از سایت ما برای سایت دیگری (مثلاً برای یک سایت ثبت آمار کاربران) ارسال می‌کنند. همچنین، اسکریپت‌ها، عکس‌ها، و غیره که از سایت دیگر به صورت http در سایت ما بارگذاری می‌شوند. مرورگر از بارگذاری و اجرای این محتواها نیز جلوگیری می‌کند. در صورتی که امکان بارگذاری این محتواها از طریق https وجود ندارد، آن‌ها از وب‌سایت خود حذف نمایید. روش دیگر این است که دو صفحه مجزا، یکی برای http و یکی برای https طراحی کنید؛ در صفحه مربوط به http، همه محتوای مورد نظر را قرار دهید اما در صفحه https، محتوای ناامن را حذف کنید. سپس در تنظیمات SSL روی سرور، درخواست‌های SSL را به آدرس صفحه https ارجاع دهید. راه‌حل دیگر این است که به جای دریافت محتوا (مثلاً عکس) از سایت دیگر، محتوا را از سایت مذکور دریافت و در منابع سایت خود قرار دهید. سپس به طور محلی آن‌ها را فراخوانی/بارگذاری کنید.
- در برخی موارد، ممکن است محتوا از سایت دیگر و با https فراخوانی شود، اما توسط مرورگر بارگذاری نشود. این مشکل معمولاً دلایل مختلفی می‌تواند داشته باشد که همگی بستگی به سرویس HTTPS سایت ارسال‌کننده محتوا دارد. مثلاً ممکن است گواهی SSL آن سایت، برای مرورگر مورد اعتماد نباشد. برای حل این مشکل، وضعیت سرویس HTTPS سایت ارسال‌کننده را بررسی نمایید.

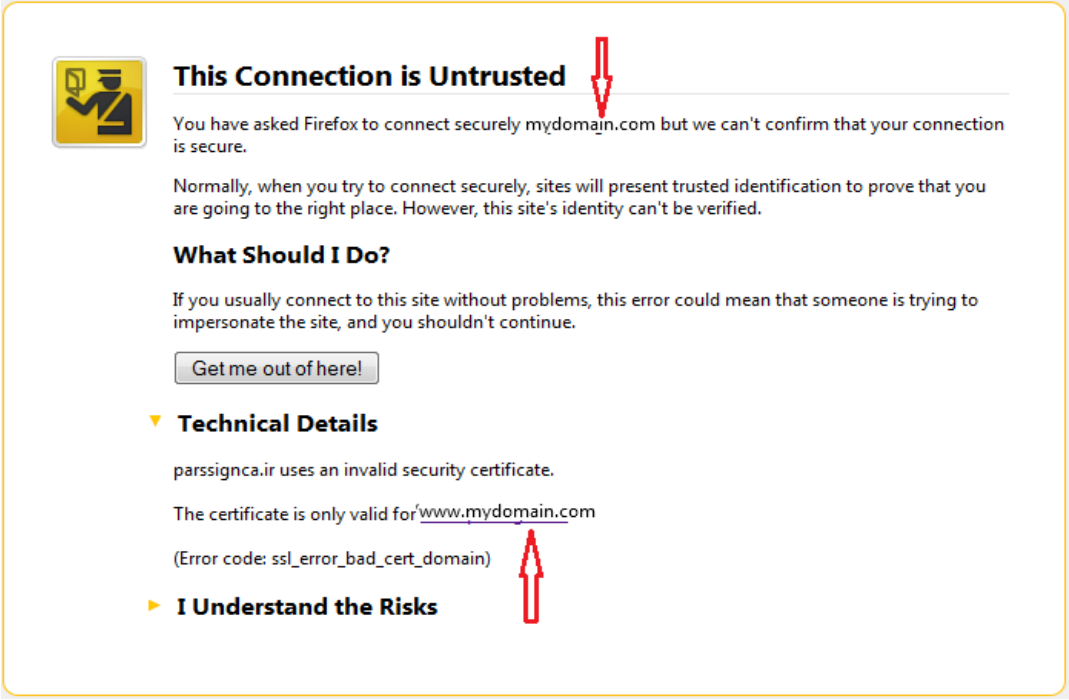
۲-۷ نمایش صفحه هشدار SSL در مرورگر

در حالت کلی این گونه هشدارها را به دقت مطالعه نموده و دلیل آن را بررسی نمایید.

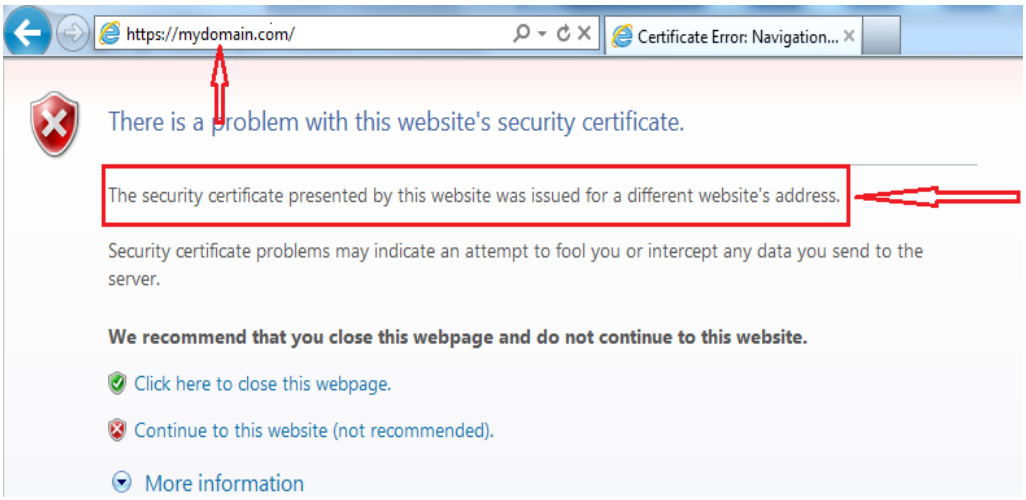
در صورتی که نصب گواهی روی سرور، همچنین نصب زنجیره روی مرورگر، هر دو به درستی انجام شده باشند اما در مرورگرها شکل‌های زیر نمایش داده شود:

- **مرورگر Google Chrome**: پیام زیر نمایش داده شود.

- **مرورگر Firefox**: پیام زیر نمایش داده شود.



- **مرورگر Internet Explorer**: پیام زیر نمایش داده شود.



دلیل مشکل فوق این است که آدرس سایت را بطور دقیق وارد ننموده‌اید. در زیر، چند سناریو که منجر به چنین خطایی می‌شوند آورده شده است:

- اگر گواهی برای www.mydomain.com صادر شده باشد اما آدرس https://mydomain.com (یعنی بدون www) را در مرورگر وارد نمایید، با صفحه خطای فوق مواجه می‌شوید. برای رفع این مشکل، یا باید همیشه آدرس دقیق وارد شود یا راه‌حل بهتر اینکه در تنظیمات سرور خود، آدرس

https://mydomain.com را به https://www.mydomain.com (یعنی با آدرس دقیق) تغییر مسیر دهید (redirect نمایید).

- ممکن است یک سایت، به چند دامنه (مثلاً mydomain.com و mydomaint.ir) تخصیص داده شده باشد. مثلاً اگر گواهی سایت برای www.mydomain.com صادر شده باشد اما آدرس https://www.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می‌شوید. در صورتی که برای یک سایت چند دامنه وجود داشته باشد اما گواهی شما فقط برای یک دامنه صادر شده باشد، باید از مرکز صدور گواهی درخواست گواهی SAN نمایید. کاربرد گواهی SAN برای استفاده از یک گواهی برای چندین دامنه است.
- ممکن است برای یک سایت فقط یک دامنه وجود داشته باشد اما در آن دامنه، زیردامنه[1] نیز وجود داشته باشد (مثلاً mail.mydomain.com). حال اگر آدرس https://mail.mydomain.ir را در مرورگر وارد نمایید، با صفحه خطا مواجه می‌شوید. در صورتی که بخواهید برای زیردامنه خود نیز از HTTPS استفاده نمایید، باید یک گواهی مجزا برای این زیر دامنه درخواست نمایید. در صورتی که بخواهید فقط از یک گواهی برای یک دامنه و تمام زیردامنه‌هایش استفاده کنید، می‌توانید درخواست گواهی Wildcard نمایید.

توجه: ممکن است صفحه‌های هشدار مشابه دیگری با دلایل خاص خود وجود داشته باشد که معمولاً مربوط به پیکربندی سرور شما می‌باشد. در صورت مواجهه با چنین خطاهایی، آن‌ها را به دقت مطالعه نموده و با انجام تنظیمات لازم روی سرور، آن‌ها رفع نمایید.

۳-۷ نمایش صفحه دیگری به جای صفحه سایت

برای استفاده از HTTPS برای یک دامنه (وب‌سایت)، باید یک آدرس IP اختصاصی (Dedicated IP Address) به آن دامنه تخصیص داده شود (رویه تخصیص IP اختصاصی در بخش ۵-۲ توضیح داده شده است). در صورتی که آدرس IP سایت با سایت‌های دیگر به اشتراک گذاشته شده باشد (Shared باشد)، هنگام درخواست HTTPS، سرور معمولاً صفحه پیش‌فرض IIS را نشان می‌دهد (زیرا نمی‌تواند تشخیص دهد چه سایتی را برگرداند).

[1] Subdomain

۴-۷ نمایش صحیح سایت HTTPS در یک مرورگر و عدم نمایش آن در مرورگری دیگر

این مشکل مربوط به گواهی SSL سایت نیست، زیرا گواهی صادرشده توسط مرکز میانی پارس‌ساین از استانداردی (استاندارد X.509) تبعیت می‌کند که وابسته به مرورگر یا سیستم‌عامل خاصی نیست. این مشکل معمولاً به دلیل استفاده از مرورگر یا سروری است که بروزرسانی نشده است. در صورتی که مرورگر و سرور هر دو به روز باشد، مشکل در تنظیمات SSL سرور است. علاوه بر بحث بروز رسانی، در برخی مرورگرها ممکن است تنظیمات SSL صحیح نباشد، لذا از این موضوع نیز اطمینان حاصل نمایید.

۸ پیوست

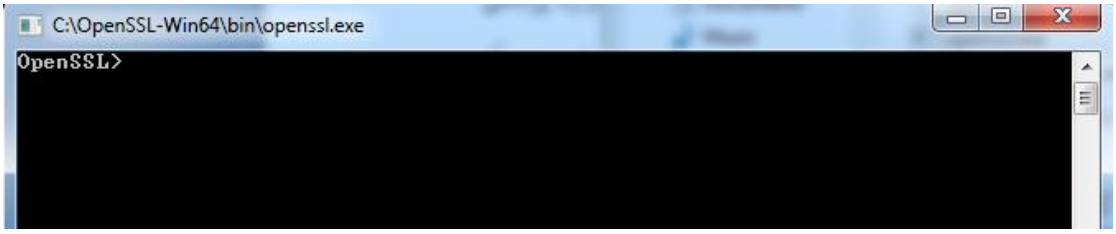
۸-۱ نحوه بررسی PEM بودن فایل کلید و تبدیل آن به فرمت PEM

برای بررسی PEM بودن فرمت فایل کلید خصوصی، آن را با یک ویرایشگر متن باز می‌نماییم. به طور مثال در ویندوز، روی فایل راست‌کلیک می‌نماییم و گزینه Open with، سپس Choose default program را انتخاب کرده و در بخش Other Programs از صفحه ظاهرشده، نرم افزار WordPad را انتخاب می‌نماییم.) در صورتی که فایل با عبارتی مشابه -----BEGIN RSA PRIVATE KEY----- شروع و به -----END RSA PRIVATE KEY----- ختم شده باشد، فرمت فایل از نوع PEM می‌باشد.

نکته: در صورتی که CSR با نرم‌افزار ParsKey Utility تولید شده باشد، فایل کلید در فرمت PEM می‌باشد.

اگر کلید خصوصی به فرمت PEM نباشد (مثلاً در فرمت DER باشد)، باید مراحل زیر را برای تبدیل آن از فرمت DER به فرمت PEM انجام دهیم:

۱. به وب‌سایت مرکز صدور گواهی الکترونیکی پارس‌ساین به آدرس www.parssignca.ir مراجعه نموده و نرم‌افزار OpenSSL را از بخش دانلود سایت دریافت نموده و روی سیستم خود نصب می‌نماییم.
۲. اگر نسخه‌ی تحت ویندوز OpenSSL را نصب کرده باشیم، به دایرکتوری bin در مسیر نصب نرم‌افزار رفته (این مسیر در ویندوز 7 نسخه ۶۴ بیتی، C:\OpenSSL-Win64\bin می‌باشد) و فایل اجرایی OpenSSL به نام openssl.exe را اجرا می‌نماییم. با اجرای این برنامه، پنجره‌ای مانند شکل زیر ظاهر می‌گردد.



۳. روبروی عبارت <OpenSSL در پنجره فوق، دستور زیر را وارد می‌نماییم:

```
rsa -inform der -in key.der -outform pem -out key.pem
```

لازم به ذکر است که اگر با لینوکس کار می‌کنیم، دستور زیر را وارد می‌نماییم:

```
openssl rsa -inform der -in key.der -outform pem -out key.pem
```

در دستور بالا، فایل key.der، فایل کلید خصوصی به فرمت DER هست که می‌خواهیم آن را به فرمت PEM تبدیل نماییم. فایل key.pem، فایل کلید جدید به فرمت PEM می‌باشد که با اجرای دستور فوق ایجاد می‌گردد.

لازم به ذکر است که برای هر یک از فایل‌های فوق، باید مسیر دقیق آن‌ها را در دستور وارد نماییم. برای مثال، در صورتی که فایل key.der را در درایو D و پوشه keys قرار داده باشیم و می‌خواهیم فایل key.pem نیز در همین مسیر ذخیره گردد، دستور به صورت زیر خواهد بود:

```
rsa -inform der -in d:\keys\key.der -outform pem -out
d:\keys\key.pem
```

در صورت استفاده از لینوکس، فرض می‌کنیم فایل‌های مذکور در مسیر home/keys/ قرار داشته باشند.

به این ترتیب، دستور زیر را وارد می‌نماییم:

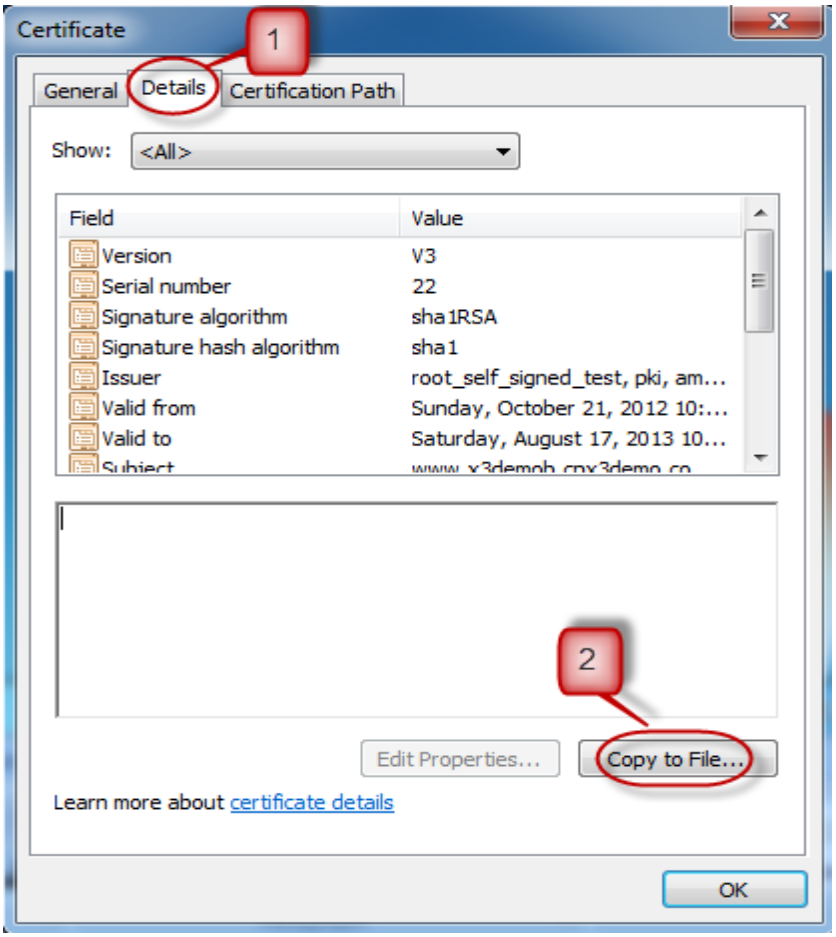
```
openssl rsa -inform der -in /home/keys/key.der -outform pem -out
/home/keys/key.pem
```

۸-۲ نحوه بررسی PEM بودن فرمت فایل گواهی و تبدیل آن به فرمت PEM

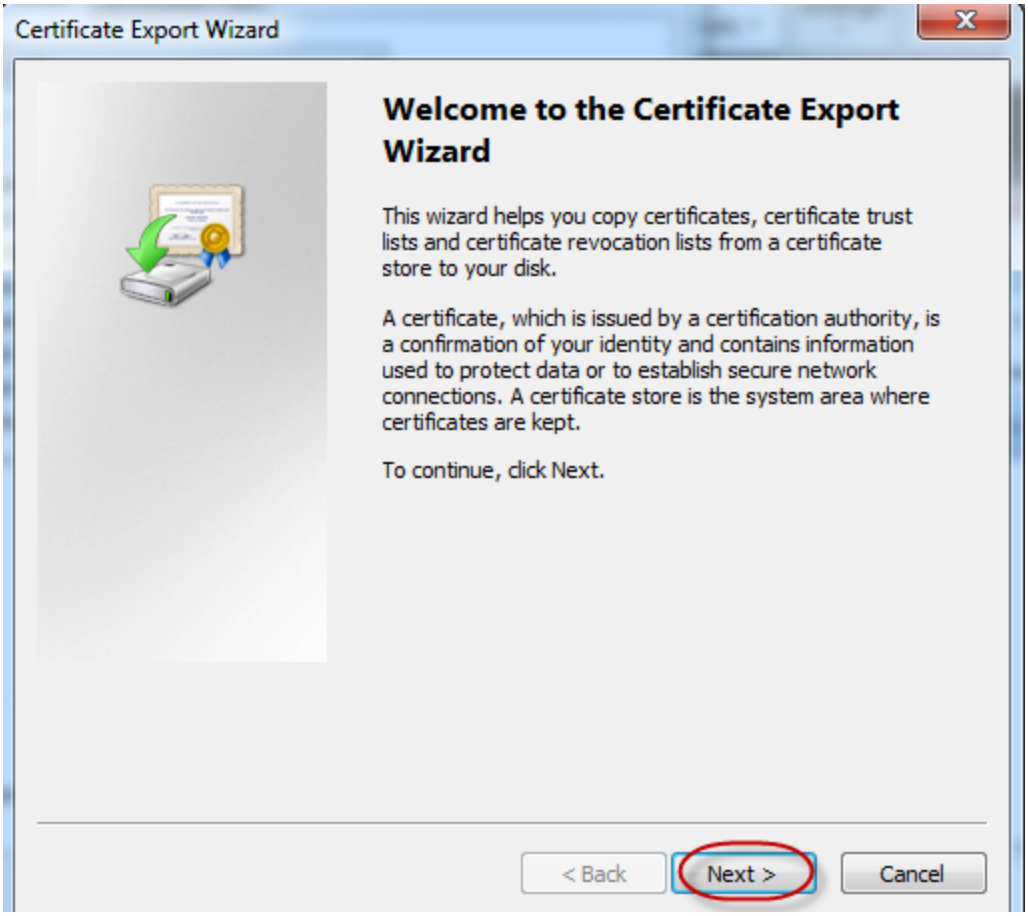
برای بررسی PEM بودن فرمت فایل گواهی، آن را با یک ویرایشگر متن باز می‌نماییم. به طور مثال در ویندوز، روی فایل راست‌کلیک می‌نماییم و گزینه Open with، سپس Choose default program را انتخاب کرده و در بخش Other Programs از پنجره ظاهرشده، نرم‌افزار WordPad را انتخاب می‌نماییم. در صورتی که فایل با عبارت -----BEGIN CERTIFICATE----- شروع و به -----END CERTIFICATE----- ختم شده باشد، فرمت فایل از نوع PEM می‌باشد.

اگر فرمت فایل pem نباشد، آن را به صورت زیر به یک فایل گواهی جدید با فرمت PEM تبدیل می‌نماییم:

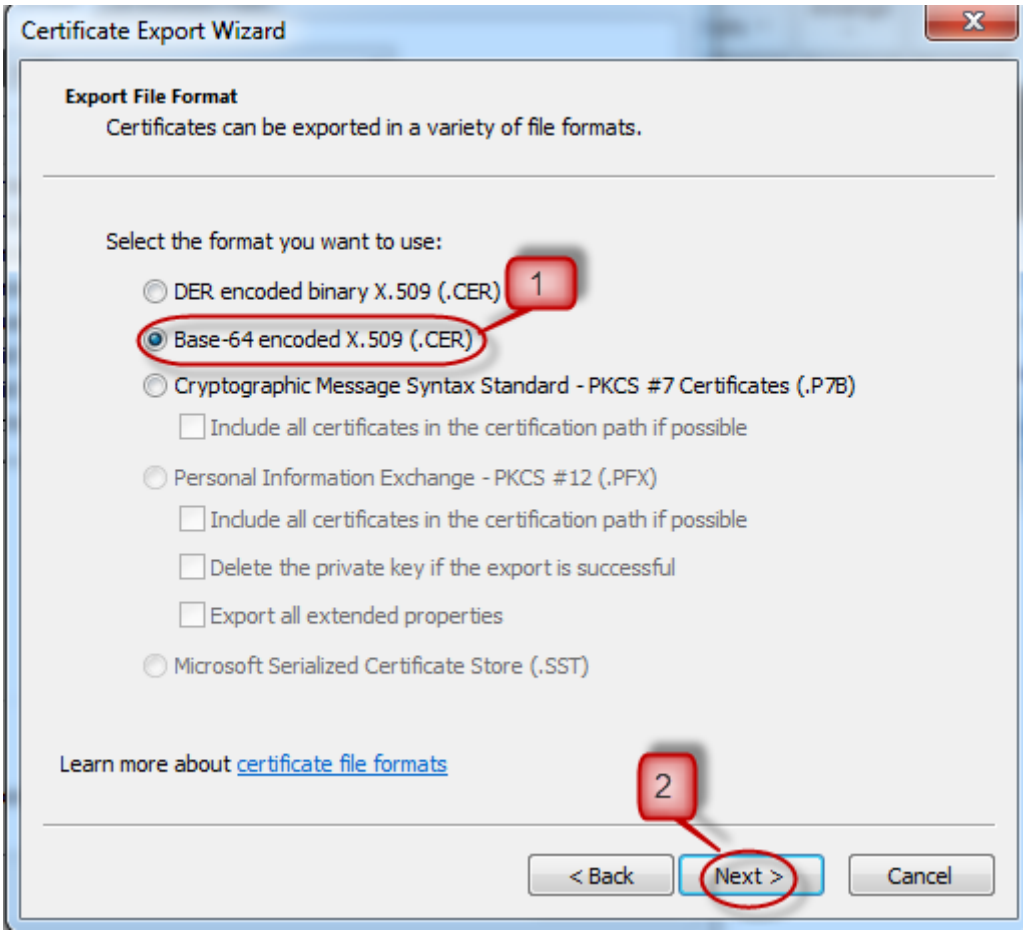
۱. ابتدا فایل مورد نظر را باز می‌نماییم. برای این کار، روی فایل گواهی دابل‌کلیک نموده، سپس در پنجره ظاهرشده روی دکمه Open کلیک می‌نماییم.
۲. در پنجره بازشده، در سربرگ Details روی دکمه Copy to Files کلیک می‌نماییم (مانند شکل زیر).



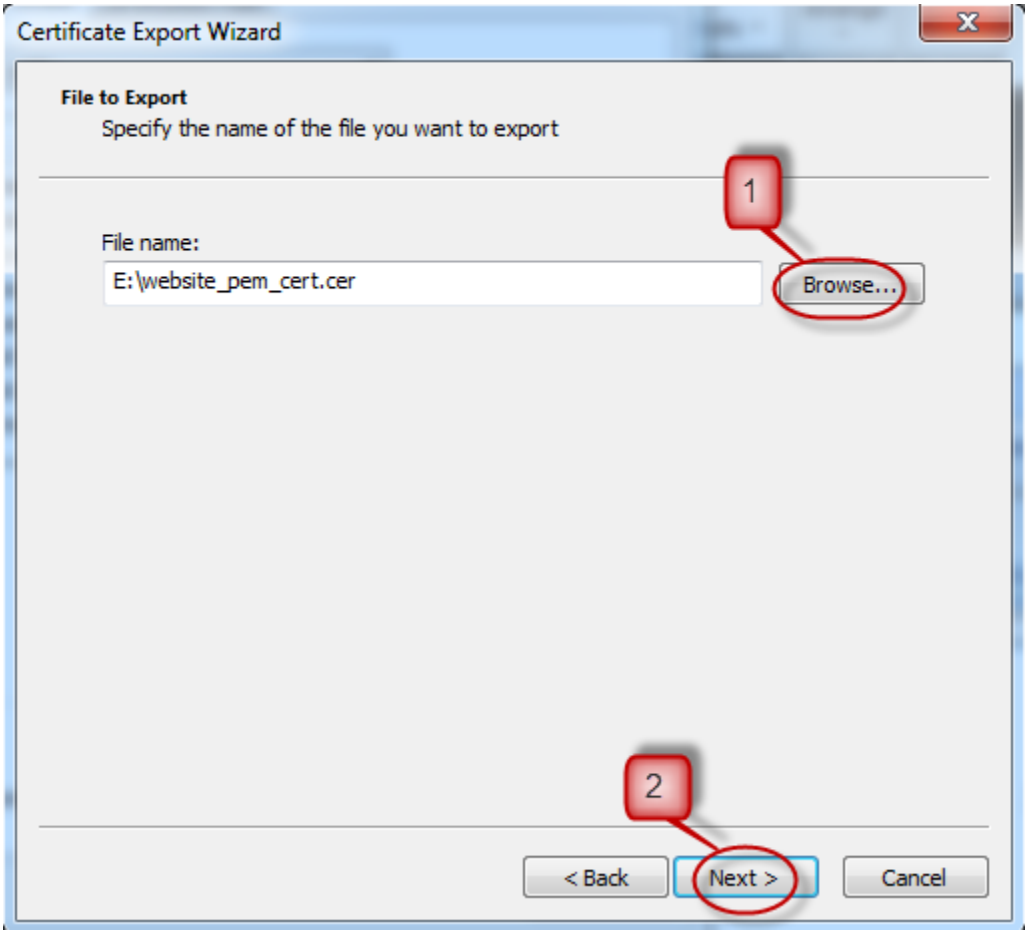
۳. در پنجره Certificate Export Wizard روی Next کلیک می‌نماییم (مانند شکل زیر).



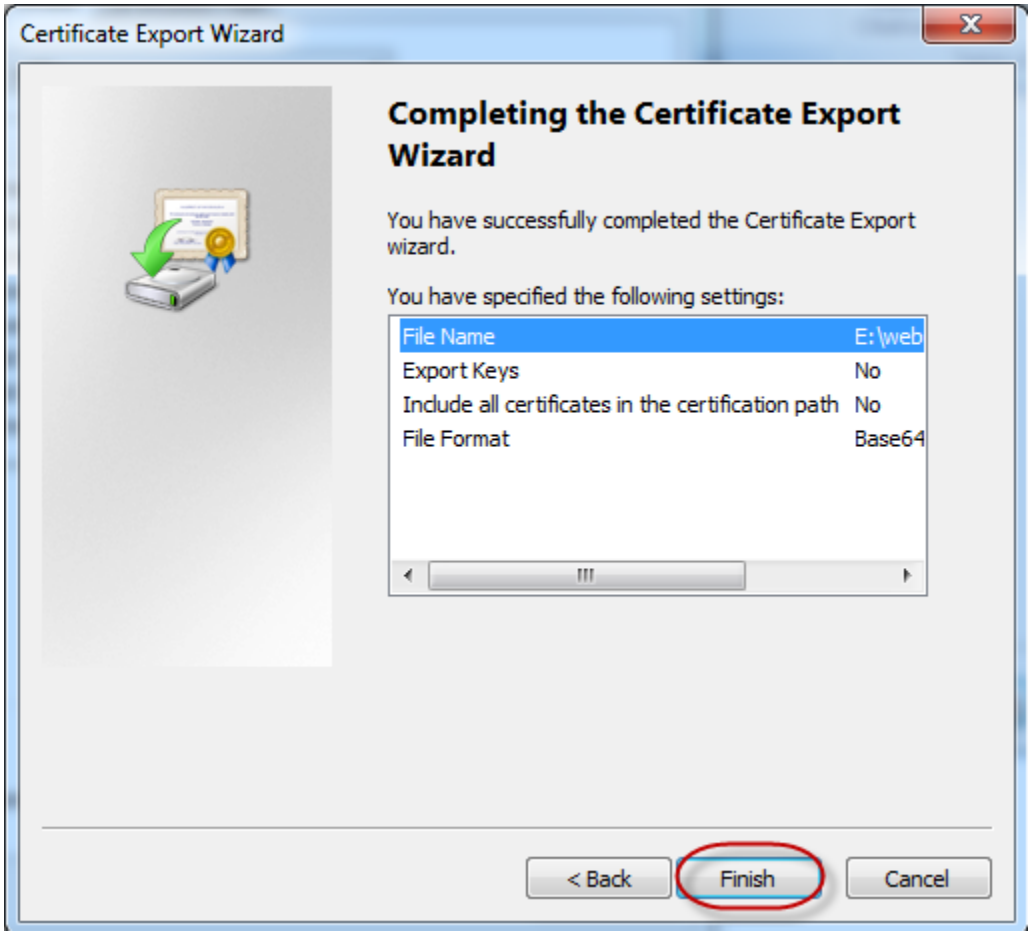
۴. در پنجره Export File Format در بخش Select the format you want to use گزینه Base-64 encoded X.509 (.CER) را انتخاب نموده، سپس روی Next کلیک می‌کنیم (مانند شکل زیر).



۵. در پنجره File to Export برای انتخاب مسیر ذخیره فایل با فرمت pem، روی Browse کلیک می‌نماییم. پس از انتخاب نام و مسیر ذخیره فایل، روی Next کلیک می‌نماییم (مانند شکل زیر).



۶. در پنجره Completing the Certificate Export Wizard روی Finish کلیک می‌نماییم (مانند شکل زیر).



۷. پنجره زیر که نشان‌دهنده موفق بودن تبدیل فایل می‌باشد، ظاهر می‌گردد. روی OK کلیک می‌نماییم. به این ترتیب، عملیات تبدیل فایل به فرمت pem پایان می‌پذیرد.